

## **Request**

Thank you for sending over your Records Management policy (retentions policy). Please can you also send over:

- 1) Information Governance Framework
- 2) Information Security Policy
- 3) Data Protection Policy
- 4) Information Rights Policy
- 5) ICT Acceptable Use Policy
- 6) Business Continuity Management Plan
- 7) E-mail Management Policy
- 8) Information Management Policy
- 9) Capacity Plan
- 10) Any other documents pertaining to the scheduling of backups for the 3 groups named below
- 11) Any other documents pertaining to the retentions of emails for the 3 groups named below

Additionally please can you send me all retentions schedule(s) applicable to these 3 groups:

- 12) The council as a whole (the corporate retentions schedule)
- 13) Private Sector Housing (any specific retentions schedule(s))
- 14) Environmental Enforcement (any specific retentions schedule(s))

## Response

Please note that all the following policies have been redacted to remove the names of officers below Assistant Director level. Names of staff are personal data, as defined by UK GDPR and the Data Protection Act 2018. Staff do not expect their names to be released to the world at large, which is the effect of disclosing information under the Freedom of Information Act 2000. As such, disclosure would breach the GDPR principles and we are withholding this redacted information under Sections 40(2) and 40(3A)(a) of the Freedom of Information Act 2000.

Q1 and Q3 to Q7 – all attached.

Q2 - The Information Security policy is being withheld from disclosure. Section 31(1)(a) of the Freedom of Information Act 2000 (FoIA) states that information is exempt information if its disclosure under this Act would, or would be likely to, prejudice the prevention or detection of crime.

Disclosure under the FoIA is deemed to be disclosure to the world at large, i.e. placing it in the public domain. The Information Security Policy is a policy aimed at staff and provides a framework for the Council's approach to reducing the risk of cyber attacks and other cyber security issues. Disclosure of the requested information to the public would be valuable information to potential cyber criminals allowing them to identify the security framework and to identify possible weaknesses in cyber security processes.

We therefore believe that the exemption at section 31(1)(a) of the FoIA is engaged for the Information Security Policy.

This exemption is subject to a Public Interest Test. Whilst the Council acknowledges the inherent public interest in transparency in its activities, it believes in this case the public interest in protecting the personal and sensitive data held on its systems is of more significance. Furthermore, the cost to the public purse of responding to cyber attacks adds to the balance of arguments against disclosure. Taking these factors into consideration, the Council assesses the public interest is not in favour of disclosure.

Q8 The Council does not hold the Information Management Policy; this is an internal Agilisys document.

Q9 Attached.

Q10 There are no further documents.

Q11 Retention of emails is subject to the E-Mail Management Policy and the three Retention Schedules attached.

Q12 Attached are the current Directorate Retention Schedules which together form the Corporate Retention Schedule. This is currently under review, but the attached are the current versions

Q13 and Q14 - There are no service specific retention schedules; these are included within the documents provided under Q12.



## Information Governance Framework

Author: [REDACTED]  
 Date: 30<sup>th</sup> September 2022  
 Version 4.0

Version Control		
<b>Document Title</b>	Information Governance Framework	
<b>Purpose</b>	To provide an accountability framework for information governance at Wigan Council	
<b>Date of Approval</b>	28 <sup>th</sup> September 2022	
<b>Valid Until</b>	28th September 2024	
<b>Owner</b>	Data Protection Officer	
<b>Approver</b>	Information Governance Operational Group (Chair – SIRO)	
<b>Distribution Method and Responsibility</b>	Intranet and Internal Comms Update (tbc) [REDACTED]	
<b>Version</b>	<b>Date</b>	<b>Comments</b>
1.0	Approved by ISWG 20 <sup>th</sup> May 2011	Issued by NetConsent 13 <sup>th</sup> October 2011
2.0	September 2019	
3.0	December 2019	Consistency with other policies
4.1	June 2022	Stakeholder consultation
4.2	August 2022	Review after stakeholder consultation
4.3	September 2022	To IGOG
4.0	September 2022	Approved by IGOG

## 1. Purpose

To provide an accountability framework for information governance at Wigan Council.

## 2. Scope

Information is a vital asset for the provision of services to the public and for the efficient management of Council services and resources. As well as rights to access public and personal information, it plays a key part in governance, service planning and delivery and performance management.

Governance is about how the Council ensures it is doing the right things, in the right way, for the right people, in a timely, inclusive, open and accountable manner.

CIPFA consider that *“Good governance leads to good management, good performance, good stewardship of public money, good public engagement and ultimately good outcomes for citizens and service users”*.

Information governance is concerned with how information is held, obtained, recorded, used and shared by the organisation. Information Governance, including physical, personal, and information security assets is an essential enabler to ensure that the Council and its partners operate legitimately, efficiently, and effectively. All associated security risks must be managed effectively, collectively, and proportionately, to ensure core regulatory and Council standards are achieved and Council actions demonstrate public accountability and confidence.

It is essential that the Council has a robust information governance framework, to ensure that information is effectively managed with accountability structures, governance processes, documented policies and procedures, staff training and adequate resources.

Ultimate responsibility for all aspects of Information Governance lies with the Cabinet and Senior Management Team. However, all officers have a responsibility to ensure that through their decisions and actions Council information assets (physical, personal, and information security) are protected in a proportionate manner.

The Council's Information Governance Framework consists of specific policy documents (detailed below) covering all aspects of information security and risks, data handling, acceptable use, and reporting protocols allied to other generic Council policies and codes.

## 3. Roles and Responsibilities

### Cabinet and Portfolio Holder

The Cabinet, also known as the Executive, is the main policy-making body of the Council and carries out Council functions that are not the responsibility of any other part of the Council, whether by law or under the constitution.

The Cabinet has overall responsibility for the strategic management and effective governance of all Council services including the strategic context in which organisational process documents are approved and establishing a scheme of governance for the formal review and approval of such documents.

The Cabinet consists of eight senior Councillors who are each 'Portfolio Holders' for a major area of responsibility and seven Lead Members who have designated responsibility. The Portfolio Holder for Resources, Finance, and Transformation has responsibilities including information, data protection and IT.

### **Chief Executive and Strategic Management Team**

The Chief Executive is the Head of Paid Service who leads the Council's staff and advises on policies, staffing, service delivery and the effective use of resources. The Chief Executive and Directors form the Council's Corporate Board, known as the Strategic Management Team, ensuring delivery of an effective Council-wide information management approach.

### **Senior Information Risk Owner**

The Council's Senior Information Risk Owner (SIRO) is the Deputy Chief Executive and Director of Resources who has overall responsibility for managing information risk in the Council. This includes ensuring:-

- that an overall culture exists that values and protects information within the Council
- that information governance compliance with legislation and Council policies
- the provision of a focal point for managing information risks and incidents
- the Chief Executive is advised of any information risk aspects and reporting annually within the Council's Annual Governance Statement

The SIRO chairs the Council's Strategic Information Governance Oversight Group and Information Governance Operational Group.

### **Caldicott Guardian**

The Council's Caldicott Guardian is the Director – Adult Social Care and Health and is responsible for ensuring that all personal/patient identifiable information handled by social care and public health services, are compliant with existing law and standards and they act to safeguard the rights of service users. The Caldicott Guardian ensures that appropriate information governance policies are in place for their services and they are adhered to by all staff and external care providers in their service areas.

### **Data Protection Officer (DPO)**

The Council's [Data Protection Officer](#) is the Strategic Lawyer – Resources (Deputy Monitoring Officer). The Data Protection Officer is a statutory role required for all public authorities by the Data Protection Act 2018 and the DPO must report to the highest management level within the Council. The DPO is required to be independent, monitor internal compliance, inform and advise on the Council's data protection obligations, approve and provide advice regarding Data Protection Impact Assessments (DPIAs)

and act as a contact point for data subjects and the regulatory authority, the Information Commissioner.

### **Information Asset Owners (IAOs)**

Each Assistant Director is an Information Asset Owner who is accountable to their Director for information systems and information assets within their service area to ensure ownership, access, usage and transfer to ensure business is transacted within an acceptable level of risk.

They are able to understand how information is held, used and shared and address risks to the information. They are also required to provide an annual assurance statement covering a wide range of information governance issues including any issues of concern during the year and how they were addressed. Each assurance statement is then submitted to the responsible Director to support their own Directors Assurance Statement that in turn informs the Council's Annual Governance Statement.

### **Information Asset Managers (IAMs)**

The ultimate responsibility for information governance sits with the Information Asset Owner (and the Director) but the Information Asset Manager can undertake the agreed processes delegated by the IAO. It is up to the IAO to determine the appropriate seniority of the IAMs in their area, but they should normally be managers who have the authority to ensure compliance by more junior staff.

### **Service Manager ICT Service Delivery**

To work with Information Governance and others to ensure the development, integration and implementation of ICT projects is managed and delivered effectively meeting the needs of technical and business stakeholders whilst managing stakeholders' expectations. To provide a productive line of communication between IG and the various ICT teams, including but not limited to security, bring into service and applications.

### **Line Managers**

All managers with line management responsibility must ensure their staff comply with all Council Information Governance policies. Staff should refer personal data breaches to them for onward reporting to the responsible Assistant Director and the Data Protection Officer.

### **All Staff**

All staff must be aware of and comply with relevant Information Governance policies and procedures. Staff is understood to include all employees, secondees, volunteers, agency staff, work experience students and any other individuals working for the Council on a contractual basis. Elected members (Councillors) are also covered by the policy.

#### 4. Corporate Information Governance Bodies

To ensure that the Council continues to maintain effective governance arrangements and related procedures across all of its activities and priorities ensuring compliance with the Data Protection Act 2018 and other privacy and information legislation, an Information Governance Operational Group (IGOG), chaired by the SIRO, has been established and meets every two months. A more strategic group – the Strategic Information Governance Oversight Group, also chaired by the SIRO – meets as required to consider any matters referred to it by IGOG.

##### Strategic Information Governance Oversight Group (SIGOG) Responsibilities

- To meet as required, at the request of IGOG or the SIRO to
  - consider negative performance trends requiring a corporate focus.
  - be advocates for and promote compliance with data protection policies across the Council.
  - support and promote the completion and maintenance of the Record of Processing Activities and Information Asset Registers in each directorate.
  - consider the implications of serious data breaches or other data incidents when there are corporate lessons to be learnt
  - review and recommend onward reporting to Strategic Management Team and/or Members.

##### Information Governance Operational Group (IGOG) Responsibilities

- To ensure that the Record of Processing Activities is maintained as the definitive record of all personal data processed by the Council and the Information Asset Register for non-personal data.
- To review, maintain and approve IG and data protection policies and procedures.
- To consider data breach, subject access and FOI notifications to the ICO, ensuring any recommendations made by the ICO are implemented.
- To take an overview of training requirements and provision in data protection and information governance matters.
- To receive performance data reports on personal data breaches, freedom of information requests and subject access requests.
- To identify trends and areas of concern for referral to SIGOG and/or SMT.

##### Audit, Governance and Standards Committee

Article 9.06 of the Council's Constitution establishes an Audit, Governance and Standards Committee. Inter alia, this committee provides independent assurance of the governance arrangements of the Council and its services which includes Information Governance. Accordingly, a report is made each year detailing the structures and processes in place to ensure compliance with data protection legislation and providing an overview of performance and key themes in personal data breaches, freedom of information and subject access requests.

This committee also receives the Directors' Annual Assurance Statement, including the Information Asset Owners' Assurance Statements confirming that the following responsibilities were followed throughout the particular financial year:-

- Managing security, compliance and risks associated with their information assets
- Carrying out an annual assessment of 'information risk'
- Maintaining Information Asset Register and Record of Processing Activities
- Ensuring that appropriate data sharing and data processing agreements are operating and DPIAs are evident in respect of new projects/contracts
- Ensuring that data is transferred securely
- Ensuring that user access rights to systems are regularly reviewed
- Ensuring that all staff have accepted all Council related policies and have completed the Council's mandatory E-learning, Cyber Security Awareness and other related courses,
- Ensuring that information security incidents are reported promptly and appropriate actions are taken to remedy data breaches and incidents
- Reviewing service specific document/information retention and disposal schedules.
- Ensuring that Freedom of Information and Subject Access requests are processed effectively
- Ensuring that business continuity management system restore priorities are managed effectively

## 5. Key policies

The key policies in the framework are the:

- [Data Protection Policy](#) – aimed at all staff to enable those working with information to have an effective understanding of their obligations regarding confidentiality and data security.
- [Information Rights Policy](#) – aimed at the public to outline how the Council and its staff deal with the public's information rights.
- [Information Compliance Policy](#) – aimed at all staff to demonstrate the policies and processes that the Council and its staff will follow with regards to information compliance, including protecting personal data.
- [Information Security Policy](#) – aimed at staff to protect the Council from cyber security issues that may have an adverse impact on the Council.

## 6. Information Governance Resources

The [Information Governance Team](#) provides expert advice and guidance to all staff on all elements of Information Governance, viz.-

- Developing the Information Governance Framework and all associated policies, standards and procedures, including integrating government and Information Commissioner specific information governance guidance, policies and codes of practice into Council policy.



- Ensuring compliance with Data Protection, Freedom of Information, Records Management, Information Security and other information related legislation.
- Processing of Freedom of Information and Subject Access Requests in accordance with legislative requirements, providing advice to services, as required
- Facilitation of the investigation of all reported data breaches to ensure Council policy is followed consistently and reporting periodically to the Information Governance Operational Group and other Governance Bodies as appropriate.
- Providing advice and guidance on all aspects of information governance and data protection to all staff.
- Supporting the Information Asset Owners and Information Asset Managers to maintain and review the Record of Processing Activities
- Providing support and guidance to all staff on data sharing and data processing agreements, data protection impact assessments and data protection contractual clauses
- Working with Council information groups and directorate teams to establish protocols and agreements on how information is to be used and shared.
- Developing information and data protection awareness and providing training sessions for staff.
- Providing support to the Council's information governance lead officers, viz.
  - a. Senior Information Risk Owner
  - b. Data Protection Officer
  - c. Caldicott Guardian
- Producing an Annual Information Governance report to Members via the Audit Governance & Standards Committee and providing other reports to Council committees on Information Governance, as required

The Chief Technology & Information Officer is responsible for the technical and cyber security management of the infrastructure and also all technical security advice.

## **7 Guidance and Associated Training**

Information Governance training for all staff will be mandatory as part of induction and delivered through the Core Learning offer.

This training will comprise two elements - (i) Data Protection and Information Governance and (ii) Cyber Security. Both will be required to be refreshed annually through the Core Learning offer.

Other training and awareness sessions on any aspect of information governance may be given to staff as required, at team meetings or other sessions provided by Directorate Management or the Information Governance Team.

Regular reminders on information governance topics are made through Team Time, corporate and local team briefings, MyTime sessions, staff news, other web-based information and/or specific emails.

## **8. Review**

This policy will be reviewed two years after approval date unless legislative, regulatory or case law changes require an earlier review.

## Data Protection Policy

Author: [REDACTED], Information Governance Policy Officer  
 Date: 28<sup>th</sup> September 2022  
 Version 4.0

### Version Control

<b>Document Title</b>	Data Protection Policy
<b>Purpose</b>	To enable those working with information to have an effective understanding of their obligations regarding confidentiality and data security.
<b>Date of Approval</b>	28 <sup>th</sup> September 2022
<b>Valid Until</b>	28 <sup>th</sup> September 2024
<b>Owner</b>	Data Protection Officer
<b>Approver</b>	Information Governance Operational Group (Chair – SIRO)
<b>Distribution Method and Responsibility</b>	Hub, Internal Comms, Cascade via IAOs [REDACTED]
<b>Version</b>	<b>Date &amp; Comments</b>
1.0	October 2011
2.0	May 2018 To take account of GDPR
3.0	May 2020 Reviewed by Information Governance team -to reflect current practice and learning from data breaches
4.1	July 2022 Biennial Review and to bring into line with other IG Framework policies
4.2	August 2022 Review after stakeholder consultation
4.3	September 2022 To IGOG
4.0	September 2022 Approved by IGOG

# Data Protection Policy

## 1. Purpose

The Council is committed to enabling those working with information to have an effective understanding of their obligations regarding confidentiality and data security. This document describes those responsibilities and provides guidelines in order to ensure that confidentiality and data security is maintained and improved when required.

## 2. Scope

This policy applies to ALL users of council email including all employees, secondees, volunteers, agency staff, work experience students and any other individuals working for the Council on a contractual basis. Elected members (Councillors) are also covered by the policy. For the purposes of this policy hereafter these groups will be referred to as 'staff'. This policy applies whilst these persons are on site and off site as the duty of confidentiality applies even where an individual is not representing the Council.

This policy relates to personal data as defined below.

### Definitions

**Personal Data** - This contains details that identify living individuals even from one data item or a combination of data items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth. Under GDPR, this now includes location data and online identifiers.

**Special Category Data** - This is personal data consisting of information as to: race, ethnic origin, political opinions, health, religious beliefs, trade union membership, sexual life and previous criminal convictions. This includes biometric data and genetic data.

For more information about special category data please refer to the [Council's Special Category Data and Criminal Offence Data Policy](#)

**Processing** – This means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

## 3. UK GDPR Principles

The principles for the processing of personal data, as set out in the Article 5 of the UK General Data Protection Regulation and incorporated into the Data Protection Act 2018, state that personal data must be:

- i. Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- ii. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
- iii. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.
- iv. Accurate and, where necessary, kept up to date.
- v. Kept in a form that permits identification of *data subjects* (i.e. living individuals) for no longer than is necessary for the purposes for which the personal data is processed.
- vi. Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Council also has a responsibility for, and to be able to demonstrate compliance with, the above principles through an accountability framework. This policy forms part of that framework.

All staff must adhere to the principles of the UK GDPR and Data Protection Act 2018 when processing personal and/or special category data and demonstrate compliance with these.

Everybody who works for Wigan Council could potentially use personal data. The Council's policy is to ensure that all personal information it obtains, uses or shares in its work is treated with care and respect, and used lawfully and fairly. The policy applies to personal data the Council processes about members and its employees as well as personal data about the public and its service users.

The Principles do **not** prevent effective working. Personal data can be obtained, used, shared and kept to provide services, look after people's interests, and support the Council's objectives. Data Protection legislation supports efficient working and reinforces the Council's objective to provide appropriate and personalised services. This policy sets out how data protection legislation applies to the Council and sets out some specific measures to assist compliance.

#### **4. Summary of Specific Measures**

All Assistant Directors (as Information Asset Owners) will:

- ensure that all staff complete mandatory e-learning training on data protection and cyber security and any bespoke practical data protection training for their service area.
- inform and seek assistance from the [Information Governance Team](#) in

advance of any new services, projects and processes involving the use of personal data, or of significant changes to existing ones. In certain cases it may be necessary to undertake a Data Protection Impact Assessment (DPIA) for 'high risk' data processing.

- report all losses, thefts or breaches of security involving personal data to the [Data Protection Officer](#) immediately (see section 25)
- ensure that staff are aware of and understand the policy.
- take steps (where practical) to anonymise personal data to mitigate against data security breaches
- notify the [Information Governance Team](#) of all new data or information sharing agreements or protocols
- participate in data protection audits
- produce and maintain a Record of Processing Activities, incorporating an information asset register
- be accountable for managing information risk and for controlling the use, protection, sharing and timely disposal of personal information.

## 5. Individual responsibility

The Council holds information about staff, service users, local residents and families and elected members.

All staff and third parties working for or on behalf of the Council, who have access to Council information in any format, via network and systems are responsible for safeguarding the personal data in their care. This carries with it an obligation to abide by this Policy, related policies and procedures and data protection and privacy legislation.

Staff cannot use personal data obtained at work for their own purposes. It is a criminal offence to knowingly or recklessly access and/or disclose personal data without the Council's permission. Anyone who uses, discusses or discloses personal data held by the Council without lawful authority is committing an offence under the Data Protection Act 2018 and individuals could face prosecution by the Information Commissioner's Office (ICO).

For staff who knowingly access, disclose or misuse Council data for their own purposes, or who knowingly ignore the requirements of this policy, then the matter will be considered and investigated under the Council's disciplinary procedure.

Serious breaches of this policy may constitute gross misconduct and lead to summary dismissal. Breaches, where applicable, may also result in civil action and/or criminal charges.

The ICO can issue fines where an organisation is unable to demonstrate compliance

with any of the principles. Fines could be anything up to £17.5 million.

## 6. Awareness and training

We will promote the need to respect privacy and confidentiality so people remain confident about using Council services. All staff who handle personal data must undertake all relevant training in data protection; mandatory training forms part of the Council's Core Learning Offer including at Induction and at regular intervals. Any queries in relation to data protection issues in the workplace should always be referred initially to Line Managers. Staff are encouraged to be proactive and ask questions if they are unsure about any issues associated with the processing of personal and/or special category data.

## 7. Obtaining information

People must be informed when we process information about them, unless there is a specific legal reason for not doing so. Any process involving the collection and use of personal data must conform to the UK GDPR principles.

Managers must ensure that the use of personal data meets these conditions and that they and their staff are familiar with the privacy notice for their own service. They should ensure this correctly identifies what personal data they collect, what they use it for and who it is shared with.

Please refer to all the Council's [Privacy Notices](#)

Any changes needed to a privacy notice should be referred to the [Information Governance Team](#).

## 8. New processes, systems and services

Departments need to be mindful of Data Protection requirements when developing or choosing a new service, process or system, and should seek advice from the [Information Governance Team](#) in order to identify the legal basis for processing personal data and to ensure appropriate data sharing/processing agreements are in place and privacy notices are updated, where necessary.

The Information Governance Team will assist with a Data Protection Impact Assessment on new initiatives or existing services or projects in any case where the impact is significant or intrusive.

## 9. Application forms and tools to gather information

Any form or process (including an automated process) designed to gather information must include a simple explanation about why that personal data is needed, and what we will do with it and refer the person to the relevant privacy notice.

## 10. Notification

The Council's notification to the Information Commissioner describes broadly how and why we use personal data; it is renewed annually every October. Departments should tell the Information Governance Team immediately about new services or projects, or

significant changes that might affect the notification.

## 11. Record Keeping

Departments must have in place adequate records management procedures, including measures to ensure that working records about people are fair, accurate, up-to-date and not excessive. Records about people must be secure, traceable and accounted for at all times. Each department must maintain an Information Asset Register and a Record of Processing Activities (which together will form part of the corporate record of processing activities and information asset register for all services) and operate a retention and disposal schedule as part of the Council's [Records Management Policy](#). Records must be disposed of securely in accordance with the retention schedule. Records management procedures, including retention and disposal, apply equally to paper and electronic records including emails.

## 12. Extent of information

Personal data must be accurate, relevant, up-to-date, adequate and not excessive. It should be easy for staff and service users to update their data. Inaccuracies must be corrected as soon as they come to light. Staff should ensure that they keep enough information to provide an effective service but avoid keeping data just in case it may become useful in the future.

## 13. Need to know

Access to personal data must only be available to those who need it. If access to data is needed only some of the time, it should only be available some of the time. Data should be used when necessary, and not purely because it is convenient to do so. This applies to all staff, including IT staff and non-technical staff with administrator or similar status. All access to systems containing personal data for maintenance or testing must be logged. Where a system has the facility to log the creation of users, this facility must be switched on.

## 14. Data Security

The [Data Protection Officer](#) must be notified of any loss, theft or accidental disclosure of personal data, or situations where this might have happened in accordance with the Serious Irregularity Reporting Protocol and/or the [Data Breach Reporting process](#), as appropriate. All premises and electronic systems where personal data is held must include appropriate security. Access to areas where information is held should be controlled. Paper files should be locked away when not in use and electronic data must be protected by adequate security measures.

It is Council policy to store data on a network server where it is regularly backed up, or with appropriate security measures, stored in the Cloud.

Personal data should not be stored on the hard drive or desktops of PCs, laptops or mobile devices. Where information is gathered and recorded through mobile working then staff should download the data onto the appropriate network server



and database as soon as a secure network connection is available and deleted from mobile devices.

Personal data should not be on display except where necessary (i.e. for operational reasons or for safety reasons).

Encryption technologies will be employed to protect the security of data including emails.

All data, physical or electronic, must be disposed of securely, in accordance with the Council's retention and disposal schedule.

## **15. Validating requests for information**

Departments must understand the legal framework that affects their work, so that they know when they have the power or the obligation to disclose information to other organisations, and to obtain it from them.

If an individual or an outside body requests personal data from the Council, the [Information Governance Team](#) must be informed so they can be properly logged and verified. Do not assume that a request from another organisation is valid just because they state it is.

## **16. Sharing Data Securely**

Information should be shared by the most secure method available. When sending information outside the Council, staff must take steps to ensure that only appropriate people will see it and they comply with the [Data Handling and Transfer Policy](#), the [E-mail Management Policy](#) and the [ICT Acceptable Use Policy](#)

## **17. Data sharing and Data Processing agreements**

A data sharing or processing agreement is required where data is being shared regularly with another party. One-off and discrete transfers do not usually require an agreement as long as a legal basis has been identified; see paragraph 15 above.

Systematic and ongoing transfers are more likely to create risks, and therefore more likely to require a formal agreement. Where the Council passes personal data to another, so that the other can perform some tasks or provide a service on behalf of the Council under contract, this should be dealt with under the contract; see paragraph 18 below.

All data sharing or processing agreements between the Council and outside agencies must be registered with the [Information Governance Team](#). Departments must not sign an agreement without seeking advice from the Information Governance Team. Agreements should be drawn up after consultation between organisations, not imposed by one on another.

## 18. Contracts

If a contract or agreement involves the processing of personal data, the contract should include measures to ensure that the data is used safely and appropriately. Standard contract clauses will detail the respective data responsibilities of both the Council and its contractors.

## 19. Access to Personal Data

Any member of staff who is asked by a member of the public for copies of data held about them should refer any such request to the Information Governance Team at [Subject Access Requests](#) so they can be logged and the individual's identity can be verified. Requests can be made verbally or in writing.

Further information for staff can be found at [Dealing with a Subject Access Request \(SAR\)](#) and in the [Information Rights Policy](#)

## 20. Complaints about personal data

If any person identifies errors or inaccuracies in the data we hold about them or points out unfair uses of their data they can ask for this to be rectified. All such requests will be logged by the Information Governance Team. Anybody wishing to use the right to rectification (or other associated rights) should follow the process on the [Council's website](#)

## 21 Data Protection Officer and Advisory Network

The Council has a nominated member of staff with specific responsibility for data protection policies, advice, training and good practice. This is the [Data Protection Officer](#), currently the Deputy Monitoring Officer/Strategic Lawyer (Resources) in Legal Services.

The Council maintains an [Information Governance Team](#) trained in Data Protection issues who are available to provide advice to staff in all areas of the council and assist the Data Protection Officer. All Directorates have a nominated Information Asset Owner (IAO) at Assistant Director level. These IAOs are accountable for managing information risk and for controlling the use, protection, sharing and timely disposal of personal information.

The Information Governance Manager is a member of the Greater Manchester Local Authority IG Expert Reference Group which meets fortnightly and provides a forum for discussion of current IG and data protection issues. The members of the group provide an extended support network for the IG Team more generally.

## 22. Confidentiality

Information explicitly accepted in confidence or as part of a confidential relationship should only be disclosed to someone else in exceptional circumstances.

Employees must not disclose confidential information to anyone else without the permission of the individual who first gave the information to them, unless the information is about serious wrongdoing or harm or there is a strong public interest/safeguarding reason or legal basis for overriding confidentiality. Advice should always be sought from the Information Governance Team if staff are unsure.

All staff have a duty to report any criminal activity or wrongdoing to the proper authorities if they become aware of it. The Council operates a [Whistleblowing Policy](#), which provides further advice on what to do in these situations.

### **23. Testing and Training**

When developing or testing any new system or process, or working on an existing system, data about real people will not be used unless it is impossible to test the system without live data. If live data must be used for testing, please contact the Data Protection Officer.

Personal data must not be used in any training exercise – real examples must be fictionalised to the point where a person cannot be identified. Personal data can only be used for training purposes where managers or supervisors need to discuss with an officer the way they handled a specific case or situation.

### **24. Monitoring and Evaluation**

The Data Protection Officer is responsible for ensuring that all departments understand the requirements of this policy and the relevant legislation. The Council's Audit Team and the Information Governance Team will periodically audit departments to ensure compliance with policies and procedures.

### **25. Data Breaches**

All losses, thefts, misuse or breaches of security involving personal data should be reported to the Data Protection Officer ([dataprotectionofficer@wigan.gov.uk](mailto:dataprotectionofficer@wigan.gov.uk)) immediately. This includes any complaint about a breach of data from a member of the public or external party. The process for handling breaches can be found [on the Hub](#). Any breach of this data protection policy should also be reported immediately to the [Data Protection Officer](#).

Thereafter, a thorough investigation shall take place and, if appropriate, will include a referral to the Information Commissioner's Office.

### **26. Review of this policy**

This policy will be reviewed two years after approval date unless legislative, regulatory or caselaw changes require an earlier review.



## Information Rights Policy

Author: [REDACTED]  
 Date: 28<sup>th</sup> September 2022  
 Version: 2.0

Version Control		
<b>Document Title</b>	Information Rights Policy	
<b>Purpose</b>	Policy framework for ensuring compliance with rights to access public and personal information in line with legislation.	
<b>Date of Approval</b>	28th September 2022	
<b>Valid Until</b>	28 <sup>th</sup> September 2024	
<b>Owner</b>	Data Protection Officer	
<b>Approver</b>	Information Governance Operational Group (Chair – SIRO)	
<b>Distribution Method and Responsibility</b>	Intranet and Internal Comms Update Internet (as aimed at general public) [REDACTED]	
<b>Version</b>	<b>Date</b>	<b>Comments</b>
1.0	Approved by Information Governance Operational Group, 19 <sup>th</sup> December 2019	
2.1	June 2022	Stakeholder consultation
2.2	August 2022	Review after stakeholder consultation
2.3	September 2022	To IGOG
2.0	September 2022	Approved by IGOG

## Purpose

To set out the policy framework for ensuring compliance with rights to access public and personal information in line with legislation

## Scope

Access to information is governed by a number of pieces of legislation, primarily the Freedom of Information Act 2000 (FOI) and Environmental Information Regulations 2004 (EIR) for public information, and the Data Protection Act 2018 (DPA) or the General Data Protection Regulation (UK GDPR) for personal information.

'Information' is used here as a collective term to cover terms such as data, documents, records and content.

'Personal information' here means any data relating to or which identifies a living individual.

'Confidential information' includes personal information, including data relating to a deceased individual, any other council information that is deemed to be sensitive or privileged in some way and should not be released or shared without safeguards in place.

Council information includes any data or information that is held by us on behalf of individuals, businesses, partners or we create in order to carry out our services.

We hold information in order to provide services to the public. Where possible we make available public information through our website, in leaflets and on demand. In many cases, information not already published can be provided on request.

We need to restrict publication of some information because it is confidential or may have a copyright attached.

We collect and hold personal information to provide services to individuals. An individual has the right to be informed about the collection and use of their personal data. We will do this by the use of privacy notices to inform individuals what rights they have and how to request them. Some rights may not be available, depending on the legal basis for processing. Legal rights available under the Data Protection Act 2018 are:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

An individual should be confident that we handle their personal information responsibly, securely and in line with good practice.

The policy will be implemented by setting standards, procedures and guidance for Council staff and guidance on access for individuals. The policy forms part of the Council's Information Governance Framework.

## The policy

### Personal information

See [Applying for your data](#)

We will handle all personal information in a safe, responsible and secure manner.

We will meet our obligations to protect personal data and the rights to privacy. This will be in accordance with the principles of Data Protection, Human Rights and other relevant data protection legislation and common law.

We will consider and address the risks to personal information when we are planning to use or hold personal information in new ways. For example, when introducing new systems, or new ways of working. This can be documented by way of a Data Protection Impact Assessment.

We will review and may take disciplinary or contractual action if staff misuse or do not look after personal information properly.

We may need to share personal information in order to perform our duties and legal obligations.

We will provide privacy notices which explain why we collect information, how we use and share information, and an individual's rights.

Individuals' rights depend on the legal basis of processing, as set out in the service specific privacy notice.

We will set out clear procedures for individuals to make requests in line with their information rights under the Data Protection Act 2018. These are most often subject access requests (SARs) when an individual is asking for copies of their personal data that has been processed by the Council but can be for other rights such as rectification.

We will normally respond to a request and provide information within one calendar month. If complex, the provision may be extended by a further two months.

We will set out clear procedures for asking for an internal review if an individual is not satisfied with our response to their request and will ensure their concerns are dealt with appropriately.

If they are not satisfied with the outcome of the internal review, they have the right to complain to the Information Commissioner's Office.

Information relating to deceased persons is not covered by data protection legislation. However, the common law duty of confidentiality still applies to the deceased person's personal information. Accordingly, requests from third parties for information relating to deceased persons will require documentary evidence that the requestor has a lawful basis to access the information and the Council will then consider whether any duty of confidentiality still remains before determining whether the information can be disclosed.

## Public information

See [Freedom of Information](#)

We wish to be an accountable and transparent Council and will publish a range of non-confidential information for the public to access and in a reusable format.

We will state if any charges or restrictions on use apply for both general and confidential information.

We will provide as much open access to our information as possible and through a Publication Scheme and a Disclosure Log of requests for public information. Wherever possible, information will be available in digital format from our website. It can also on request be available in printed formats.

We will set out clear procedures for requesting general information and we will respond as promptly as possible and normally within 20 working days.

We will set out clear procedures for asking for an internal review if the requestor is not satisfied with our response and will ensure their concerns are dealt with appropriately. We will normally respond to the request for a review within 20 working days.

If an individual is not satisfied with the outcome of the internal review, they have the right to complain to the Information Commissioner's Office.

## Responsibilities

Wigan Council is the overall body responsible for providing information, with the legal obligations being enforced by the Information Commissioner and the courts.

Specific responsibilities for all staff within the council are as follows:

- Awareness of the relevant legislation relating to requests for public information and an individual's information rights for their personal information
- Understanding and adhering to this policy and related information governance policies and procedures.

All Wigan Council managers are responsible for the implementation of this policy within their teams.

## Review

This policy will be reviewed two years after approval date unless legislative, regulatory or caselaw changes require an earlier review.



## ICT Acceptable Use Policy

Author: [REDACTED], Information Governance Policy Officer  
 Date: 28th September 2022  
 Version 3.0

### Version Control

<b>Document Title</b>	ICT Acceptable Use Policy
<b>Purpose</b>	To regulate acceptable use of all IT equipment, facilities and services to protect the Council from data loss, unauthorised access and cyber-crime
<b>Date of Approval</b>	13 <sup>th</sup> September 2021
<b>Valid Until</b>	31 <sup>st</sup> August 2023 (biennial review)
<b>Owner</b>	Director of Digital Services and Integration
<b>Approver</b>	Information Governance Operational Group (Chair – SIRO)
<b>Distribution Method and Responsibility</b>	Intranet Hub and Internal Comms [REDACTED]
<b>Version</b>	<b>Date &amp; Comments</b>
1	April 2018 Final iteration of previous policy owned by Assistant Director, ICT Strategic Partnerships
2	September 2021 Full scale review; approved in principle by Information Governance Operational Group, 9 <sup>th</sup> September 2021; approved by Data Protection Officer, 13 <sup>th</sup> September 2021.
3.1	July 2022 Minor changes to include references to Cloud storage and web-based mail
3.2	September 2022 To IGOG with queries/suggestions from [REDACTED]
3.0	September 2022 Approved by IGOG



## 1. Purpose and Scope

1.1. Wigan Council is a recognised Digital Council and encourages the wide scale use of its ICT Systems, Technology and Services for communicating with residents, clients, and other parties for business related purposes.

1.2 The aim of this policy is to clearly communicate what Wigan Council considers to be acceptable use of all IT equipment, facilities and services by users (see definition in 1.4 below) in all circumstances and environments and thereby protect the Council's/residents' information from loss, unauthorised access, and cyber-crime.

1.3 This policy applies to **all** ICT equipment/technology and media used to conduct Council business between both internal and external services/organisations including, but not limited to, PCs, VDIs, laptops, 2-in-1 Laptops, tablets, smartphones (including council funded SIM cards), all software, all cloud services, all storage media, all network resources, all land line devices, all social media and all on-line meetings.

1.4 This policy applies to everybody who is an authorised user of the Council's network or the Council's Information Management systems irrespective of the system or network being accessed and whether that access is from a Council building or from a remote location. The term user includes, but is not limited to, staff (whatever their contract terms), elected members, contractual third parties and agents of the Council who have access to the Council's system without exception.

1.5 This policy should be read in conjunction with the following suite of policies and protocols

- [BeWigan Behaviours](#)
- [Employee Code of Conduct](#)
- [Information Governance Framework](#)
- [Connectivity Guide](#)

## 2. Golden Rules

You must: -

2.1 only use authorised software and applications approved by ICT.

2.2 use Council-provided IT equipment, services and systems for business purposes only.

2.3 take care of Council devices, use equipment safely, securely, and efficiently in a professional manner being vigilant to cyber threats and physical theft of information or a device.

2.4 dispose of and transfer council devices and other IT resources through the Council's IT Service without exception

2.5 comply with all associated policies and protocols, including but not limited to, those within the [Information Governance Framework](#) (in particular the [Email Management Policy](#)), the [Employee Code of Conduct](#) and the [Connectivity Guide](#)

- 2.6 understand your data protection and privacy responsibilities and accordingly complete all Council mandatory training requirements in this area.
- 2.7 be aware of your Cyber Awareness responsibilities and always undertake the training that is shared with you by the Council.

### 3. Information Security

You must:-

- 3.1 be fully aware of, and understand, the Council's [Information Security Policy](#) noting in particular the need to
- 3.2 protect all of your system and network access passwords against any misuse.
- 3.3 **never** share your password
- 3.4 only use your network credentials to access Council networks or home working environments in line with the [Connectivity Guide](#)
- 3.5 protect information on your devices by ensuring all Council devices are kept in a secure place, never leaving them unattended and using lock screen when not in use.
- 3.6 exercise caution in on-line meetings in respect of sharing information and personal data with third parties
- 3.7 ensure any printed Council information is disposed of in line with the [Confidential Waste Policy](#)
- 3.9 report immediately any suspected security incident, including loss/theft of equipment or potential data breaches using the process available at [Suspected Irregularity Reporting Protocol](#), [IT security](#) (loss/theft) or [How to handle a data breach](#) (personal data breach)

### 4. Access to Systems

You must:-

- 4.1 only access/attempt to access Information Management systems/files that you have been authorised to access and only for official Council purposes.
- 4.2 never upload or store personal and other sensitive data in a cloud storage facility (third party internet site) not provided by the Council unless we have a data sharing agreement with the third party and the transfer of data has been approved by the relevant Information Asset Owner (IAO). Advice from ICT on potential security risks must be sought and ICT agreement to allow access following an appropriate technical and security assessment must be obtained and reported to the IAO prior to approval.
- 4.3 **not**, under any circumstances, use Council systems to access information about family, friends, neighbours.
- 4.4 **not** use Council systems to access information about colleagues unless this is for official council purposes.
- 4.5 **not** access any Council system with an account other than the account that is your own and registered in your own name.
- 4.6 only access Council systems and devices from secure networks in line with the [Connectivity Guide](#) and [Working Differently Protocols](#)
- 4.7 follow the [Connectivity Guide](#) if "Tethering" to a mobile device for long periods of time, in particular the requirement to inform line manager and Audit
- 4.8 connect Council devices and other portable devices on a frequent basis to the Council network including to the council's remote working platform (currently at least once each week) to enable important IT security and operational updates to be applied to your device.

4.9 understand not connecting a Council device to the Council network for longer than 30 consecutive days will result in the device being disabled

## 5. Remote Working

You must:-

5.1 always comply with the detailed requirements of the [Connectivity Guide](#) and [Working Differently Protocols](#)

5.2 never connect a Council device to unsecure wifi - tethering should be the first form of connectivity in non-council buildings unless this is at home

5.3 seek prior Management approval to “tether” to any Council mobile device and therefore utilise its mobile data allowance

5.4 have an appropriate personal WIFI provision when working from your home (any use of Council mobile data when working from home must be pre-authorised by the relevant Assistant Director and is only permissible for short periods of time)

5.5 any working outside the UK must have the explicit agreement of the Assistant Director

## 6. Internet Usage

You must:-

6.1 only use the Internet for business purposes

6.2 **not** access sites containing, or distribute content which relates to, terrorism, pornography, racist, obscene or otherwise offensive material

6.3 comply with the Council's [Social Media Policy](#)

## 7. Confidentiality

You must :-

7.1 always observe your duty of confidentiality in line with the [Employee Code of Conduct](#)

7.2 **not** access files or data you have not been authorised to access without exception irrelevant of system or platform

7.3 **not** copy or transmit data outside the Council except as authorised by the requirements of your role

7.4 must encrypt personal data if it is being transmitted beyond the Council in line with the [Email Management Policy](#)

## 8. Monitoring

The Council is responsible for all Council owned devices and the data held on them. Accordingly, the Council reserves the right to monitor Council communication systems and services. This includes, but is not limited to, email, electronic messaging, internet and social media, system access, mobile data usage. The Council operates appropriate Firewall and Filtering technologies to fulfil this responsibility.

## 9. Review

This policy will be reviewed two years after approval date unless legislative, regulatory or case law changes require an earlier review.

# **BUSINESS CONTINUITY MANAGEMENT POLICY**



## **Document Control**

<b>Organisation</b>	Wigan Council
<b>Title</b>	Business Continuity Management Policy
<b>Prepared by</b>	Health Protection and Civil Contingencies Team
<b>Owner</b>	Governance & Information Security Working Group
<b>Subject</b>	Business Continuity Management

<b>Document Approvals</b>		
Version	Sponsor Approval	Date Approved
1	Corporate SMT	10 <sup>th</sup> May 2016
1	Cabinet	14 <sup>th</sup> July 2016

<b>Document Distribution</b>		
Version	Date Distributed	Distribution Method
1	31/10/16	Intranet & Internal Communications

<b>Revision / Review History</b>		
Revision / Review Date	Previous Version Ref	Description of any Revisions

## Contents

<b>Section</b>		<b>Page</b>
<b>1</b>	<b>STATEMENT</b>	<b>4</b>
<b>2</b>	<b>Definition of Business Continuity and Management</b>	<b>5</b>
<b>3</b>	<b>Aim</b>	<b>5</b>
<b>4</b>	<b>Objectives</b>	<b>5</b>
<b>5</b>	<b>Scope</b>	<b>6</b>
<b>6</b>	<b>Requirement and Standards</b>	<b>6</b>
<b>7</b>	<b>Methodology</b>	<b>8</b>
<b>8</b>	<b>Triggering - Invoking Business Continuity Plans</b>	<b>9</b>
<b>9</b>	<b>Responsibilities</b>	<b>11</b>
<b>10</b>	<b>Command and Control Structure</b>	<b>13</b>
<b>11</b>	<b>Business Continuity Management in the Community</b>	<b>14</b>
<b>12</b>	<b>Review</b>	<b>14</b>
<b>Appendix 1</b>	<b>Plan Do Check Act Cycle applied to Business Continuity Management Systems and Process</b>	<b>15</b>

## **1. STATEMENT**

- 1.1** This Policy sets out Wigan Council's commitment and direction to Business Continuity Management, to safeguard the delivery of its services to the residents of the Borough as a result of a disruptive event, or events, occurring.
- 1.2** Disruptive events do occur, they usually happen without warning and range in size and severity. They could be caused by: severe weather; a fire; loss of a utility supply; industrial action; a Pandemic outbreak, such as Swine or Avian Influenza; or a contractor ceasing to operate. Such events may affect our staff, ICT networks, buildings and our critical infrastructure and thereby our ability to deliver the services we provide in the usual way. They could even cause the suspension of some services. While all services are important, during the subsequent continuity and recovery phases the Council will direct resources to those which have been deemed essential/business critical services first.
- 1.3** The Business Continuity Management strategy and framework that supports this Policy enables the council to: develop plans at corporate; directorate and service area level to mitigate against disruptive events; increase its ability to protect and maintain its core business critical functions and services and recover from disruptive events, as quickly as possible. It also reflects both the Council's statutory duties and good practice.
- 1.4** The Council's Senior Management Team will lead and develop a culture whereby Business Continuity Management is an integral part of business planning at corporate, directorate and service area level.
- 1.5** The Council will exercise its Business Continuity Management Plans at corporate, directorate and service area level annually, to test their effectiveness, promote awareness, ensure staff are familiar with their roles during an interruption to normal service and the relevance of business continuity management to operational practice; as part of the continual improvement cycle.
- 1.6** The Business Continuity Management Policy has links with:
- The Councils Risk Policy and its Risk Register
  - The Council Emergency Plan
  - The Greater Manchester Community Risk Register

## **2.0 Definition of Business Continuity and Management**

**2.1** Business Continuity (BC) is defined as the capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident. *(Source: ISO 22301:2012)*

**2.2** Business Continuity Management (BCM) is defined as a holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. *(Source: ISO 22301:2012)*

**2.3** It is a comprehensive management process that systematically analyses the organisation, identifies threats and builds capacity to respond appropriately to them.

**2.4** The immediate response to a disruption is a key component of businesses continuity management. However, its prime focus is on maintaining and recovery of business functions in a priority order following the disruption.

## **3. Aim**

**3.1** The Aim of this policy, supporting strategy and framework is to:

- Provide the structure for maintaining council priority services in the event of disruption.
- Ensuring the welfare, safety and security of its staff, their environment and members of the public who use those services.
- Develop an approach which can be extended to link with partner agencies and wider community to enhance overall resilience within the Borough.
- Provide a flexible structure for the overall response.

## **4. Objectives**

**4.1** The main objectives are to:

- Promote awareness of the importance of effective BCM both in relation to WMBC-related services, and also from a Borough resilience perspective
- Minimise the risk of disruption to council services and service users, through careful planning.



- Respond effectively to an incident/emergency.
- Outline the triggers, co-ordination/command and control arrangements for responding to an incident/emergency.
- Maintain, as far as possible, those council services identified as essential/business critical functions, while responding to the emergency
- Restoring all council services disturbed during an incident/emergency, by priority, in a structured way and within agreed recovery timescales.
- Communicate with staff, elected members, suppliers, partners and the public during an emergency; where appropriate advise the public of any risks.
- Develop a culture of resilience leading to positive and proactive responses to adverse situations.
- Comply with the duties under the Civil Contingencies Act 2004 and follow best practice.

## **5. Scope**

**5.1** Business Continuity Management is a borough wide activity; therefore this policy applies to all; services within the council; staff; internal and external stakeholders; resources and business processes. This includes multi-agency/partnership working, any commercial activities, procurement, suppliers, service partners and outsourcing of services – this is not an exhaustive list.

## **6. Requirement and Standards**

**6.1** In addition to making sound business sense for any organisation, the Civil Contingencies Act 2004 places a statutory duty upon the Council, as a Category 1 responder, to:

- Maintain plans to ensure services continue to be delivered in the event of an emergency, so far as is reasonably practicable;
- Assess both internal and external risks;
- Have a clear procedure for invoking business continuity plans;
- Exercise plans and arrange training for those who implement them;
- Review plans and keep them up to date; and
- Advise and assist local businesses and organisations with their Business Continuity Management arrangements.

**6.2** Business Continuity Management arrangements are effective only if specifically built for the organisation. The Council's programme is aligned with the principles of:

- ISO 22301: Societal security - Business continuity management systems –Requirements
- ISO 22313: Societal security - Business continuity management systems –Guidance

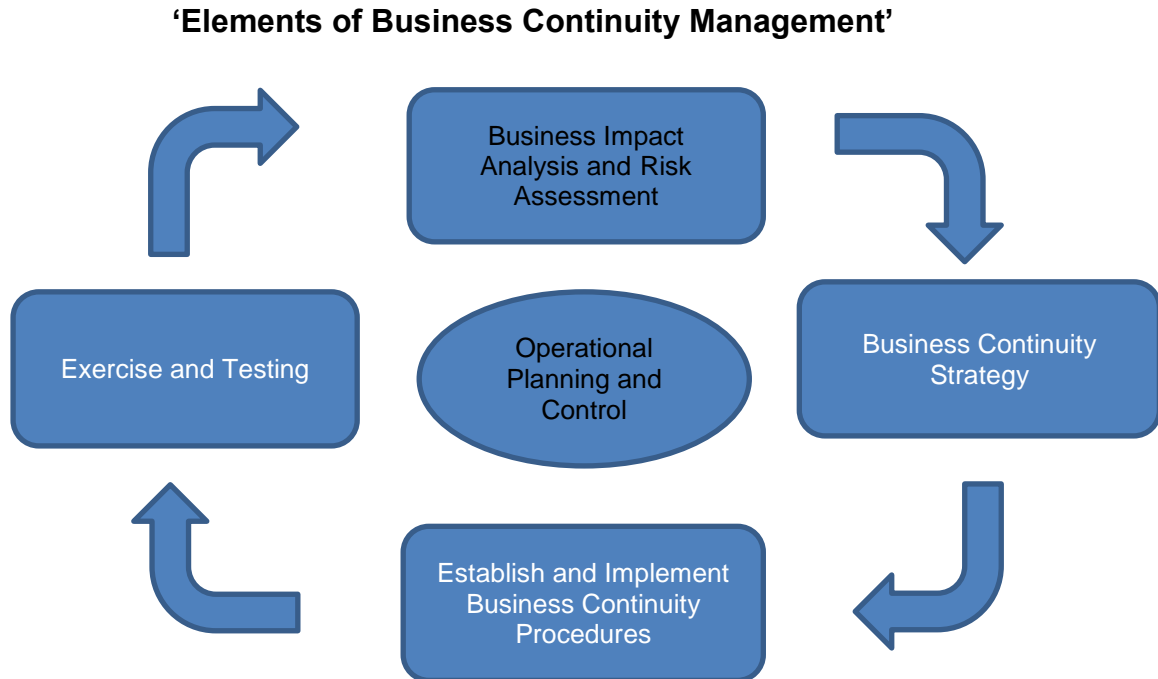
this is reinforced by reference to the Business Continuity Institute's Good Practice Guidelines and other best practice.

**6.3** The Councils ICT service will ensure that the requirements and standards set out in the ICT contract in relation to Business Continuity Management are complied with, tested and maintained throughout the life of the contract in accordance with the contractual requirements; the contractor will supply evidence of this to the council's Assistant Director Strategic ICT and Partnerships, or nominated representative, in accordance with the requirements of the Contract and specifically Schedule 8.6 (Business Continuity and Disaster Recovery Plan).

**6.4** Property will often play a significant role in business continuity in relation to ensuring adequate accommodation for staff during and after an incident. The council is moving to a Corporate Property Management (CPM) model, which once fully implemented will mean that one team is responsible for managing all council buildings. This will allow Property Team to co-ordinate the property requirements in relation to a business continuity issue. However, up until the point that CPM is fully operational the Property team would liaise with any relevant services about property implications.

## 7. Methodology

7.1 ISO 22313 applies component parts/elements to the Business Continuity Management life cycle; the model is best illustrated and described through the 'Elements of Business Continuity Management' as shown below:



*(Source: ISO 22313: Clause 8.1.1 - Elements of BCM)*

7.2 The Council's approach to Business Continuity Management seeks to embed it within the culture of the council, whereby it is an integral part of business planning at corporate, directorate and service area level. On going training, education, awareness raising, including ownership and leadership by the council's Senior Management Team is critical to this.

7.3 The Council will use the approach of the 'Plan, Do, Check, Act cycle' as applied to the 'Business Continuity Management System and Process' outlined in ISO 22301 and ISO 22313, illustrated in Appendix 1. The key stages are:

### Plan

- Establish business continuity policy and objectives.

### Do

- Develop suitable controls and procedures.
- Undertake Business Impact Assessments of Service Areas and key contracts.

- Consider the risks identified in the Corporate Risk Register and Greater Manchester Community Risk Register.
- Develop Business Continuity Plans for critical services.
- Review Business Continuity arrangements for key contracts.
- Record Business Continuity Plans and ensure copies are easily accessible.
- Train staff responsible for activating, managing and delivering a plan.
- Communicate with partners and the wider business community.
- Invoke Plans as required.

### **Check**

- Annual desktop/walkthrough test of Business Continuity Plans.
- Periodic exercise of Plans.
- Quality review of Business Continuity Plans by Internal Audit.
- Survey of business community on their preparedness for significant business interruptions

### **Act**

- Undertake analysis of incidents that have required invocation of a Business Continuity Plan.
- Update Plans with identified gaps/improvements, as a result of activation or testing.
- Update Plans in response to events or emerging risks.
- Provide feedback and assurance to the Council's Cabinet and Audit, Governance and Improvement Committee.

## **8. Triggering - Invoking Business Continuity Plans**

**8.1** Business Continuity Plans may be activated by a variety of internal or external disruptive events occurring or threatened.

**8.2** Disruption which cannot be dealt with through normal operational procedures by a service will trigger the invoking of the Service Area Business Continuity Plan by the Service Manager or their deputy.

**8.3** Where the disruption impacts on a number of services within a Directorate, or a single service is in danger of being, or has been overwhelmed, the Directorate Business Continuity Plan will be invoked by the Director or Assistant Director.

**8.4** The Corporate Business Continuity Plan will be activated:

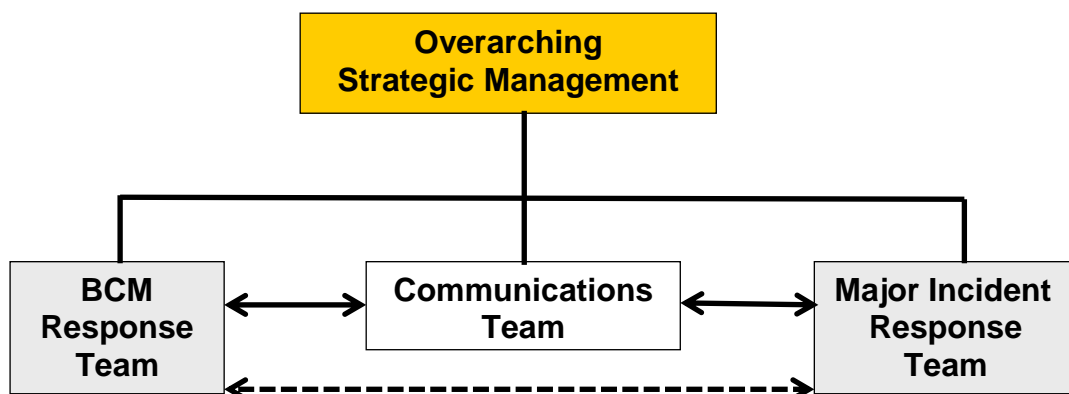
- during normal working hours by the Chief Executive or the Deputy Chief Executive;
- outside normal working hours by the Senior Duty Officer on Call;

if there is 'Corporate Level Disruption' or it is threatened; this could be triggered:

- If the disruption cannot be dealt with by the implementation of a limited number of Service Area and/or Directorate Business Continuity Plans;
- Special arrangements need to be implemented by the Council in order to deal with the disruption;
- A co-ordinated corporate response is required;
- An issue is likely to cause widespread disruption to the majority of council services;
- The Council's Chief Executive or Deputy deem it necessary to respond to the disruption.

**8.5** Depending on the circumstances the Council's Major Incident Plan may also be activated; if not already triggered by the incident. This will require the following points to be considered:

- Overarching Strategic coordination of the Major Incident and the Business Continuity Management incident/emergency;
- Separate but coordinated Tactical arrangements;
- Business Continuity Management Response Team liaison with the Major Incident Response Team and vice versa;
- Impact on partner organisations.



## **9. Responsibilities**

**9.1** This policy forms part of the Risk Management Policy which is reviewed by the Governance & Information Security Working Group and the Audit, Governance and Improvement Review Committee on an annual basis.

**9.3** The Governance & Information Security Working Group will provide a forum for the monitoring and review of business continuity arrangements; the BCM part of the agenda will be jointly Chaired by the Director Resources and Contracts (Deputy Chief Executive) and Director of Public Health (Chief Officer with responsibility for Civil Contingencies) .

**9.4** The council's Senior Management Team will be responsible for ensuring:

- The identification of corporate critical services and contracts, and undertaking business impact analysis of those services;
- Corporate Business Continuity Plans are in place for critical services and contracts;
- Corporate Business Continuity Plans are kept up to date and reviewed annually;
- The embedding of a Business Continuity culture throughout the organisation and its key stakeholders.
- The development of wider resilience across the business community.
- Plans are tested annually by a structured desktop/walkthrough and periodic exercising of Plans;
- Lessons learned from testing, exercising or the activation of Plans are shared and used to improve them.

**9.5** Directors will ensure their Assistant Directors will be responsible for:

- The identification of Directorate critical services and contracts, and undertaking business impact analysis of those services;
- Directorate Business Continuity Plans are in place for critical services and contracts;
- That Directorate Business Continuity Plans are kept up to date and reviewed annually;
- The embedding of a Business Continuity culture throughout their Directorate
- The selecting and appointing a Business Continuity Champion to represent their Directorate on the Business Continuity Management Steering Group
- Plans are tested annually by a structured desktop/walkthrough and periodic exercising of Plans
- Liaison with external stakeholders to build a more resilient operating environment across the Borough.
- Lessons learned from testing, exercising or the activation of Plans are shared and used to improve them.

**9.6** Assistant Directors will ensure their Service Managers will be responsible for:

- The identification of Service Area critical functions and contracts, and undertaking business impact analysis of those services;
- Service Area Business Continuity Plans are in place for critical services and contracts;
- That Service Area Business Continuity Plans are kept up to date and reviewed annually;
- The embedding of a Business Continuity culture throughout their team;
- Their staff understand and are familiar with their roles when Plans are invoked;
- Plans are tested annually by a structured desktop/walkthrough and periodic exercising of Plans;
- Staff and resources are released, as required to support the invoking of other Service Area, Directorate and Corporate Business Continuity Plans, as directed by senior management;
- Lessons learned from testing, exercising or the activation of Plans are shared and used to improve them.

**9.7** The councils devolved procurement resources will ensure Business Continuity arrangements are considered in the contractual arrangements for critical services, supplies or outsourcing of services delivered on behalf of the council. Guidance and co-ordination will be provided by the Procurement Commissioning and Contract Management Group.

**9.8** The Public Health Protection and Civil Contingencies Team will have responsibility for facilitating and delivering training about Business Continuity across the Council, as agreed by the Governance & Information Security Working Group and assist in the exercising of plans, providing linkages with external responding agencies as appropriate.

**9.9** The Public Relations Team will have responsibility for all external communications with and messages to the public, partners, suppliers and other external agencies during the activation of any Business Continuity Plan; as contained within the activated plan or agreed by senior management.

**9.10** HR & OD services will have responsibility for internal communications and messages to staff when any Business Continuity Plan is activated either by sharing information as contained within the activated plan or as agreed by senior management. Directors and Assistant Directors will support the sharing of messages as and when required. The web team are also responsible for supporting the internal communications function to share key messages with staff online where necessary.

**9.11** Internal Audit will monitor compliance with this policy and provide assurance on the effectiveness of business continuity arrangements through an on-going programme of audit reviews across the Council.

## 10. Command and Control Structure

### **Strategic**

The purpose of the Strategic level is to consider the incident in its wider context; determine define and communicate the overarching strategy and objectives for the incident response; authorise expenditure; establish the framework, policy and parameters for lower level tiers; and monitor the context, risks, impacts and progress towards defined objectives; determine if mutual aid is required from other authorities or assistance required from other agencies – give media interviews as appropriate.

### **Tactical**

The purpose of the Tactical level is to provide liaison between Strategic and Operational levels; provide appropriate advice on tactical issues to Strategic and Operational level; ensure that the actions taken by the Operational level are co-ordinated, coherent and integrated, in order to achieve maximum effectiveness and efficiency in line with critical functions; ensure effective liaison with media and partner agencies.

### **Operational**

The purpose of the Operational level is to implement Service Area Business Continuity Plans; collate information and provide situation reports as requested; Manage and deliver critical services, in line with Corporate, Directorate and Service Area Business Continuity Plans; Assist and support other Service Areas.



## **11. Business Continuity Management in the Community**

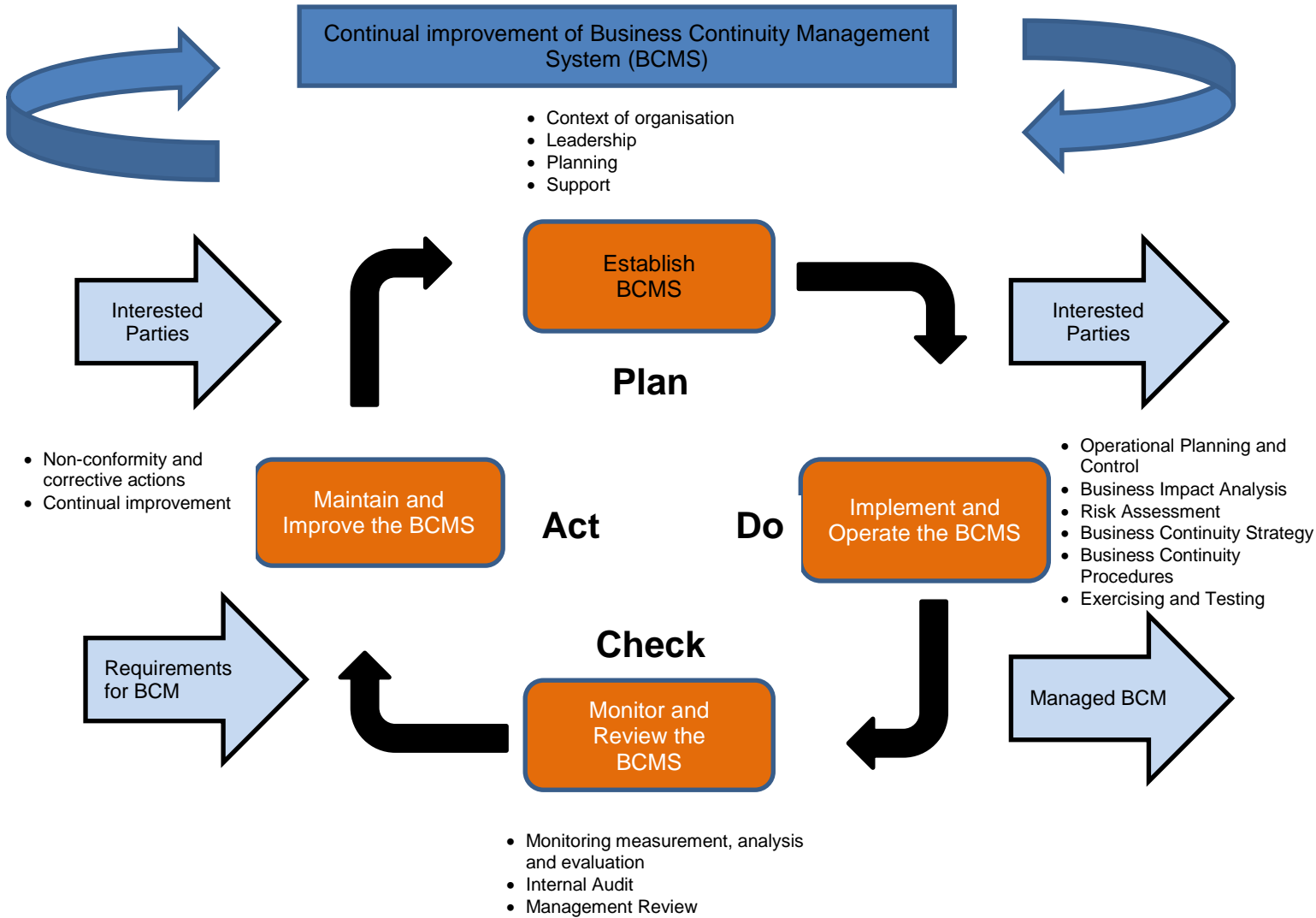
- 11.1** The Council will provide advice and guidance to the community via its website, other appropriate mediums/forms and by the provision of links to other organisations websites that provide advice, guidance and highlight best practice in relation to Business Continuity Management.
- 11.2** The council will work with partners to promote Business Continuity Management in the community and participate in appropriate practitioner groups/forums.
- 11.3** On the invocation of the Corporate Business Continuity Management Plan, consideration needs to be given as to whether the situation is impacting on partner organisations (e.g. severer winter weather). An understanding of the respective positions is needed to enable mutual support to be mobilised as required. A prearranged confirmation with key partners to establish a Common Recognised Information Picture (CRIP) will assist in maintaining integrated resilience and responding capabilities. The Council is best placed to instigate and coordinate the conference call (this will require maintaining a full contact detail listing, with reservists, for all partner organisations).

## **12. Review**

This policy will be reviewed annually by the Governance & Information Security Working Group, or as required, and the Group will submit a report following any review to the Audit, Governance and Improvement Review Committee.

# Appendix 1

## Plan Do Check Act Cycle applied to Business Continuity Management Systems and Process



(ISO 22301: Clause 0.2 and ISO 22313)

## Email Management Policy

Author: [REDACTED], Information Governance Policy Officer  
 Date: 30<sup>th</sup> June 2022  
 Version 3.0

### Version Control

<b>Document Title</b>	Email Management Policy
<b>Purpose</b>	To set out all users' responsibilities when dealing with email
<b>Date of Approval</b>	07/07/2021
<b>Valid Until</b>	07/07/2023 (biennial review)
<b>Owner</b>	Data Protection Officer
<b>Approver</b>	Information Governance Operational Group (Chair – SIRO)
<b>Distribution Method and Responsibility</b>	Hub, Internal Comms, Cascade via IAOs [REDACTED]
<b>Version</b>	<b>Date &amp; Comments</b>
1.0	October 2017 Governance & Information Security Working Group and SMT
2.0	July 2021 IGOG
3.0	June 2022 Amendments re email deletion policy

# Email Management Policy

## 1. Introduction

- 1.1 Email and Instant Messaging (IM) are an essential part of the way we do business. Email should not be treated as an extension of the spoken word because their written nature means they are treated with greater authority. As well as taking care over how email messages are written it is necessary to manage email messages appropriately after they have been sent or received.
- 1.2 All email messages are covered by the information and personal data rights established in the UK General Data Protection Regulation (GDPR), Data Protection Act 2018 (DPA), Freedom of Information Act 2000 (FoIA) and Environmental Information Regulations 2004 (EIR) and can also form part of the corporate record. Messages sent via email can result in legal action being taken against the Council or individuals and can be used as evidence in legal proceedings.
- 1.3 The Policy was developed with the Council's Information Governance Operational Group (**IGOG**).
- 1.4 There are several reasons why as a Council we cannot continue to store indefinitely all of the emails that have ever been sent or received. Firstly, personal data should only be retained as long as is necessary to fulfil the purpose of the data processing. This is one of the principles of the UK GDPR and indefinite storage would be contrary to that principle. Secondly, storage is both finite and costly. The demand for more electronic storage is increasing our IT service costs and additional charges will continue to be incurred unless action is taken to reduce the volume of electronic records being held. Finally, the vast number of emails currently held has meant that responding to FOI and Subject Access requests can be burdensome in terms of time and cost.

## 2. Purpose

- 2.1 This email policy sets out all users' (as defined in paragraph 3.2) responsibilities when dealing with email and requires that emails are:
  - used only when this is the most appropriate form of communication
  - drafted with care and attention.
  - transmitted securely, where appropriate, adhering to the council's use of encrypted email and O365 tools.
  - filed in the relevant record system but only if content needs to be retained, and not retained for longer than is necessary and in accordance with each Directorate's Data retention schedule/policy.
  - removed from Email folders on a regular basis in line with the Council's Data retention policies whether that be manually governed or automated through system archiving inclusive of O365.
- 2.2 There are two main sections within the policy: the first focuses on sending messages and the second focuses on managing messages that have been sent or received. All users should ensure that they are familiar with the content of the policy and use it as a point of reference when dealing with email. To ensure staff and elected members are familiar with the content of the policy the authority will provide support and advice where requested about the policy and keep staff aware of any changes that are made.

## 3. Scope

- 3.1 This policy applies to ALL users of council email including, but not limited to, staff (whatever their contract terms), elected members, contractual third parties and agents of the Council who have access to the Council's system without exception.
- 3.2 Email in its entirety, messages received by and sent from stand alone, network, portable, virtual

Wigan Council platforms and devices.

- 3.3 All emails prepared and sent from Wigan Council email addresses or mailboxes, and any non-work email sent using Wigan Council ICT facilities is subject to this policy.
- 3.4 All Council emails sent are subject to the council's Microsoft "DLP" Data Loss Prevention monitoring process.
- 3.5 This policy also covers the storing of emails in network folders in line with the council's Data Protection and IT Security Policies.
- 3.6 Access to colleagues' mailboxes is covered in this policy. Permission should be sought from an Assistant Director or above and the reasons should be clear. The period of access should be kept to a minimum. A job needs to be logged with the IT Self-Service portal to allow access.
- 3.7 Leavers' mailboxes and staff transferring between services or departments are covered by this policy.

## 4. Using email

### 4.1 When to use email

Email is not always the best way to communicate information. Email messages can be misunderstood either in tone or substance. Replies can also be cursory as people often have a large number of emails to process. The decision to send an email should be based on a number of factors including:

- **The subject** –email messages can be used for different types of communication and can constitute a formal record of proceedings. The types of communication which email can be used for include general business discussions, disseminating information, agreement to proceed and confirmation of decisions made. Although email can be used for these types of communication, it may be necessary to consider whether the sensitivity of the information would be more appropriately communicated in a different way.
- **Recipient's availability** – if a message needs to be passed onto a person in the same office, speaking to them face to face might be more productive or sending them an instant message, particularly if they receive large volumes of email. If the person to whom the message is being delivered is not located in the office it might be better to phone them, depending on the subject or nature of the communication. You should continue to monitor the matter, even after sending an email to someone, to ensure it is picked up and a response (where required) is given and appropriate action is taken.
- **Speed of transmission** email messages are a good way of transmitting but email is a Fire and Forget Technology. Most emails are delivered very quickly but email should not be relied on where the immediacy of delivery is important. Where the recipient is expecting the information, follow up with a quick call if appropriate based on priority. Where information needs to be communicated as a matter of urgency it is better to use the telephone, video call or Instant Messaging via the Council's communications platforms.
- **Speed of response** \_although email messages can be sent and delivered quickly and read or acted upon immediately, one of the perceived advantages of using email is that it can be responded to at the recipient's convenience. However, where an immediate action or response is required, it may be better to speak to the person directly and send email confirmation if it is deemed to be necessary.
- **Number of recipients** –although email is often considered to be a good way of disseminating

information to large groups it should be noted that the Council's default email setting is limited to a maximum of 300 recipients. The ability to send an email to everyone in the Council is restricted to the Comms Team and the Executive Support Officers. If a message needs to be conveyed to everyone at the Council the message should normally be placed on the Intranet or the Council's Internal Communications team should be contacted and requirements discussed with them.

Non-corporate email systems should not be used unless prior permission from the Council's communications team, Information Governance team and IT team has been collectively given in advance.

## 4.2 Email Content

As noted above, email is potentially disclosable under access rights laid down in data protection law and the Freedom of Information Act. It is therefore important that emails are handled with the same care and attention that is given to other business correspondence.

Emails should be drafted carefully, using appropriate business language, and time should be taken to review the content of an email before it is sent. It is important that consideration is given to the way in which the message is being conveyed. This includes thinking about the title, the text and the addressees. Also, when discussing an individual or family, be mindful of the fact that the content of the email may constitute personal data about them and they may be entitled to a copy of it if requested.

Emails should be brief, polite and factual. Personal comments or judgements should not be included in emails. This applies to both internal and external emails.

Always consider a recipient's and a sender's reasonable expectations of privacy with respect to their email address. Do not automatically include all recipient addresses in the "To:" or "Cc:" message headers or forward emails that contain the sender's or other people's email addresses, without deleting those addresses first. When sending an email to more than one recipient always check whether any of the recipients have a private email address rather than a business email address and if so ensure that the blind copy (BCC) function is selected.

**ALL** users with access to council email are expected to observe **ALL** Data Loss Prevention messages once warned when sending emails externally.

All external emails have a disclaimer at the footer of the email to protect the Council from information being disclosed to unauthorised personnel. However, there is no guarantee that this will protect individuals from potential legal action if emails sent include unsupported allegations, sensitive or inappropriate information.

Email fonts should be in line with the Council's [style guide](#) and follow all Accessibility guidelines.

## 4.3 Managing Dialogues

Email messages should be restricted to one topic to make them easier to file and manage. If another matter needs to be discussed with the recipient then a new message should be created. Similarly, if the subject changes significantly within a message string then a new string should be created by changing the title when responding.

Where a recipient to an email message includes an external third party or a different service, the entire content of the email string should be checked and any legal advice, sensitive or unnecessary personal data or irrelevant information removed before replying to or forwarding the message.

#### 4.4 Sensitive Information

The privacy and confidentiality of the messages sent via email cannot be guaranteed. Once an email leaves the protection of the Council's network on its way to an external email address, it is travelling over the internet which is an unsecure network. This means that someone with the knowledge and capability to intercept your email could read its contents. It is the responsibility of all senders to exercise their judgement about the appropriateness of using email when dealing with sensitive subjects.

The use of **Recall** cannot be relied upon to remove all emails in the event of a sensitive email being incorrectly sent to the wrong recipient(s). Recall only works when the email has been sent to user's desktop and has not been opened. However, many users' emails are also pushed to mobile devices such as iPad and mobile phones, where the recalled email will still be visible.

Consequently, the recipient may not see the recall message before opening the previous version. It is therefore essential that if you do send an email incorrectly to the wrong recipient(s), that you send a further email, as soon as possible, advising the recipient(s) that they have been sent information which they should not have access to and advising them to delete the email without reading. Staff are duty bound not to read/access personal information which they do not need to know, so should be aware that they should not do this, in the same way that they would ethically not read somebody else's letters/documents if they were lost or misaddressed.

**Email encryption** should be used in **ALL** circumstances for emails that contain personal and/or sensitive information sent to **external** email addresses, except where the external email domain is on the trusted organisations list, so that it ensures they are sent securely, reducing the risk of data loss and helping us comply with data protection legislation. You should use the approved encryption facility for any emails to external addresses when the contents of your email or any attachments within it include personal data, confidential information or business sensitive information.

Instructions on who is on the trusted organisations list and how to use email encryption to encrypt your emails can be found here <http://thehub/OurCouncil/Internal-services/IT/Security/Secure-email.aspx> on the council's intranet.

Where **Automatic email** is being sent by systems and the content includes personal and/or sensitive data then this must be approved by the Information Asset Owner (usually the Assistant Director for the Service) and this must be brought to the attention of the Information Governance Operational Group so that a risk assessment can be carried out and an exception to the policy can be applied if appropriate.

#### 4.5 Large File Transfer

To protect network performance, the file size of an email is restricted to 20MB. If you are sending large volumes of data that are likely to exceed this limit, you will need to use an alternative transfer method as provided below.

**Internal emails** – If an email is likely to include file attachments which exceed 20MB, then instead of sending this information by email you should instead email a link to a network file share location or a shared workspace such as SharePoint or Microsoft Teams.

**External emails** – Where emails exceeding 20MB are to be sent externally you should use the **Egress Switch Large File Transfer** (LFT) function. This enables you to send large files securely by uploading them to hosted Cloud storage and then sending recipients a link from which they can download the file. This option is located on every council desktop and is identified by the Egress shortcut.

Instructions on how to use the LFT facility can be accessed on the intranet.

## 4.6 Use of Microsoft Teams for Instant Messaging/Chat

Microsoft Teams allows instant messaging and presence.

This feature enables all staff with Council network accounts to communicate directly with each other using instant messaging, voice-to-voice calls or video conferencing. This facility is not intended to replace traditional email but is an additional communication tool which allows users to quickly check information or arrange both short notice and planned meetings. Care must be taken when using the platform for communicating financial information, authorisations, decisions or other information.

Whilst instant messaging is a tool which can aid collaborative working and communication, it should not be used in such a way that interferes with others' job responsibilities.

Bear in mind that IM is also a corporate record covered by the information and personal data rights established in the UK General Data Protection Regulation (GDPR), Data Protection Act 2018 (DPA), Freedom of Information Act 2000 (FoIA) and Environmental Information Regulations 2004 (EIR).

When communicating via Microsoft Teams (voice or video) calls, and information of a personal or sensitive nature is being discussed, staff must be aware of their surroundings and ensure appropriate steps are taken to safeguard the security of the information being disclosed.

A comprehensive **Office 365 Policy** is being developed.

## 4.7 Misuse and personal use

Email is primarily a business tool for the purposes of work and users should avoid sending personal emails, storing personal data within mailboxes and giving out their work email address for personal matters. Bear in mind managers have the right to access your mailbox in order to monitor your activity, investigate any allegations of misuse or to check communications when you are on leave. Any personal or social communications should be limited or directed towards IM. It should be noted that email messages can constitute a formal record and can be used as evidence in legal or disciplinary proceedings and may be shared with HR and trade unions for such purposes. Email messages may also be disclosable to the public under information rights. Be careful, therefore, to be fair and accurate when communicating information.

***The Acceptable Use of IT Policy*** provides further information about what constitutes acceptable use of our ICT Systems, Technology and Services.

## 4.8 Security

Computer viruses can be easily transmitted via email and internet downloads. To protect the email network email messages are routinely scanned to ensure they do not contain viruses. Please be aware of your responsibility to keep the council safe from Cyber Attacks and make sure the emails you receive are not of "Phishing" type. Check the sender's email address and the look and feel of the email. If the email doesn't feel right then report it using the "Report" function within the email message itself. Using this function will remove the email from your mailbox and report to the IT Service desk for additional investigation.



Incoming email messages that are suspected of containing viruses will be held by IT. An email will be sent to the intended recipient informing them that the message has been held and giving them



details of who sent the message. The email message and the attachment will be retained by Agilisys for a month before being deleted.

Although IT Services are required to keep virus software up to date, it is the responsibility of all email users to safeguard against accidental virus transmissions. These can be avoided by not opening attachments, clicking links or downloading programs if you do not know where they originated from.

If you are concerned that an email you have received may have a virus you should refer it to the IT Service Desk, Supportworks.

## **5. Managing Mailboxes**

### **5.1 General Housekeeping**

Everyone should routinely and regularly review emails in their mailbox. Messages that are no longer required or have been saved on a case management system or in another appropriate location should be deleted; this applies to Sent Boxes, Personal Folders and Deleted Items as well as In Boxes. Doing so will mean that work can be conducted more effectively as it will help in locating all the information relating to specific areas of business. It will also aid searches of mailboxes, for example when locating records for compliance with the Freedom of Information Act or Subject Access Requests.

Email messages will constitute a record if they contain information relating to business transactions that have happened or are going to take place, decisions taken in relation to the business transaction or any discussion that took place in relation to the transaction. For example, during the decision to put out a tender document for a particular service, background discussion about what this should and should not include might take place via email and should be saved as a record in an appropriate case file location. Emails must be stored in the relevant records management system as soon as possible and retained in accordance with the Directorate's document retention schedule.

Email is a communication tool and should not be routinely used as a records system.

### **5.2 Storage and Retention**

Email messages will be automatically deleted from your Inbox, Sent Items, and personal folders four years after their received date. To prevent loss of information, email messages which are business records must be acted upon and moved to an appropriate location as quickly as possible.

If required for legal, forensic audit or investigative purposes, a deleted email can be restored within that four-year period, but not beyond. Email recovery requests will require the approval of an Assistant Director or above.

Due to the low business value of Instant Messaging, IM conversations should not be routinely retained or archived.

### **5.3 Leavers**

Leaver mailboxes are the responsibility of managers and requests to delete them should be raised as part of the leaver process. A plan for retention of important email content should be agreed with managers and those staff that are leaving and an exit discussion form should be completed. Leaver mailboxes, if not deleted, are still capable of receiving email long after staff have left. Managers are solely responsible for managing this process and raising a leaver form to delete leavers' mailboxes within 3 months of exit from the authority, unless there is good reason to retain it for longer. This 3 months allows for the mailbox to be managed and any data that needs to be retained by the service to be retrieved. This can be

extended but only by an additional 3 months and only when there is a specific agreed reason that access to a leaver's mailbox is required for longer.

Should failure to close down a leaver's mailbox lead to a data breach or other irregularity, then disciplinary action may be taken against those responsible for managing the mailbox. The forms for managing leavers are available here <http://thehub/MyEmployment/Self-service/Employment-forms.aspx>

Please understand your responsibilities.

## 5.4 Movers

Movers will retain their mailbox and email address so should be careful to ensure that they make those corresponding with them aware of their move and that emails no longer relevant to their new role are redirected. Staff should ensure that they inform those they regularly deal with that they are moving and provide alternative contact details to ensure they do not continue to receive emails that are no longer relevant to them. An exit discussion form should be completed. The forms for managing movers/transfers are also available here: <http://thehub/MyEmployment/Self-service/Employment-forms.aspx>

Staff transferring between services or departments must have their shared inboxes reviewed by their manager to ensure that future access is only to inboxes where a business reason is established. Access to inboxes no longer justified must be removed and a job request should be raised via the Self Service portal.

## 5.5 Making your mailbox manageable

There are a number of approaches that you should follow to aid the management of email messages. These include:

- Allocating sufficient time each day or week to clean up your mailbox
- Emptying deleted email messages from the "Deleted Items" folder
- Dealing with ephemeral or temporary items first e.g. calendar items, Out of Office messages etc
- Promptly delete low value, non-record messages which are no longer needed for reference purposes from the inbox and sent items folders
- Deleting unsolicited junk email or spam without reading them
- Using publish and point links to shared workspace areas such as Sharepoint or MS Teams rather than sending documents to multiple users
- Identifying which emails are records and mark or highlight them so they can be moved to the appropriate record system
- Deleting email messages that are kept elsewhere as records or where responsibility for saving them lies with the sender.

## 5.6 Saving Emails and Attachments

In order to prevent loss of information, emails must be acted on and moved to an appropriate location as quickly as possible.

It is not necessary to capture every email in an email conversation string separately. Instead, email should be saved in case management and record systems at key points during the conversation, when key decisions are made and transactions are processed.

Email attachments should be saved as part of a record, in order to provide context to an email. However, there will be occasions when it won't be necessary to save both the email and its attachment - for example, if an attachment has been sent for reference purposes only and you know it has been captured elsewhere.

When saving emails, the Outlook Message Format Unicode (.msg) should be used in order to ensure that the saved email is a true representation of the email as a record and retains the characteristics of the original email.

## 5.7 Responsibility for Keeping Email Records

As a general rule, the responsibility for saving and keeping an email record should be observed as follows to avoid duplication of records:

For internal email records sent or received:

- The sender or initiator of the dialogue forming a message string is responsible for keeping the record
- If action is required by recipients, or the recipient is responsible for keeping the record on the matter communicated, they should also keep a copy

For email records sent externally:

- The sender is responsible for keeping

For external email records received:

- If received by one person then the recipient is responsible for keeping
- If received by multiple recipients, then the person responsible for the area of work relating to the message is responsible for keeping

The decision matrix at Appendix A provides a guide to determining which email messages should be saved as a business record.

## 5.8 Shared mailboxes

In the case of shared mailboxes, management is likely to be shared between everyone who has Access. As is the case for individual mailboxes, the purpose in managing a shared mailbox is to identify emails that should be retained as a record of an activity and save them within the appropriate system. Any ephemeral or temporary messages should be deleted at the earliest opportunity.

When managing shared email mailboxes, there will also need to be some additional rules relating to when to delete an email message from the mailbox, how to identify an email message as having been answered and the types of email messages that should be treated as records. While it is the responsibility of the owner to ensure that there are specific rules relating to the management of shared mailboxes it is the responsibility of everyone with access to shared mailboxes to abide by those rules.

It is important to remember that any email that made a significant contribution to the discussion of the business being conducted should be saved as a record and not just the final conclusions. The discussions that take place in the mailbox folder will represent the context within which the final decision was made and must be maintained as a record of the proceedings.

## 6. Review

This policy will be reviewed two years after approval date.

## Decision Matrix for Email Record Management

### Sending Emails

	Yes	No
1. Does it relate to work?	Go to Qu.2	Email is personal and can be deleted
2. Am I sending an email to another member or members of staff that requires action?	<b>Save email</b> as a business record	Go to Qu.3
3. Am I sending an email to another member or members of staff which authorises a piece of work?	<b>Save email</b> as a business record	Go to Qu.4
4. Am I sending an email to an external recipient which is business related correspondence?	<b>Save email</b> as a business record	Go to Qu.5
5. Am I forwarding an email I received in which I am requesting an action?	<b>Save email</b> as a business record	Go to Qu.6
6. Am I forwarding an email I received just for information?	Email is for information only and is therefore short term. Auto delete or delete earlier once no longer required	Go to Qu.7
7. Am I replying to an email sent by an external recipient	<b>Save email</b> as a business record	

### Receiving Emails

	Yes	No
1. Does it relate to work?	Go to Qu.2	Email is personal and can be deleted
2. Was the email sent by a member of staff?	Go to Qu.3	Go to Qu.5
3. Was the email sent for information purposes only i.e as a BCC or CC?	No need to save. Email is a business record and should be saved by the originator	Go to Qu.4
4. Was email a reply to one I had sent and contains further information or action?	<b>Save email</b> as a business record	Go to Qu.5
5. Was the email from an external source?	<b>Save email</b> as a business record	



## Capacity Plan

<b>Document Classification:</b>	<b>Agilisys Internal</b>
<b>Document Ref.</b>	<b>IMS-DOC-A12-3</b>
<b>Version:</b>	<b>1.1</b>
<b>Dated:</b>	<b>12 April 2021</b>
<b>Document Author:</b>	<b>[REDACTED]</b>
<b>Document Owner:</b>	<b>[REDACTED]</b>

### Revision History

Version	Date	Revision Author	Summary of Changes
1.0	04/01/2019	[REDACTED]	Initial Draft
1.1	12/04/2021	[REDACTED]	Annual review – minor update

### Distribution

Name	Title
[REDACTED]	Service Director

### Approval

Name	Position	Signature	Date
[REDACTED]	Service Director		12/04/2021

## Contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>3</b>
1.1	SCOPE OF THE PLAN .....	3
1.2	METHODS USED .....	3
1.3	ASSUMPTIONS MADE.....	3
<b>2</b>	<b>CURRENT AND FORECAST DEMAND FOR SERVICES .....</b>	<b>4</b>
2.1	CHANGES AFFECTING CAPACITY REQUIREMENTS .....	4
2.2	TRENDS .....	4
<b>3</b>	<b>SERVICE AND RESOURCE SUMMARY AND RECOMMENDATIONS.....</b>	<b>5</b>
3.1	SERVICE UPGRADES REQUIRED.....	6
3.2	IMPACT OF NEW TECHNOLOGIES AND NEW TECHNIQUES .....	6
3.3	OTHER RECOMMENDATIONS .....	6

## List of Tables

<i>TABLE 1 - CURRENT CAPACITY USAGE .....</i>	<i>5</i>
<i>TABLE 2 - SERVICE UPGRADES REQUIRED .....</i>	<i>6</i>

## **1 Introduction**

This capacity plan addresses the capacity needs of Bolton and Wigan Partnership and the current ability of the infrastructure to meet them. It makes recommendations for adjusting current capacity in line with future requirements before any thresholds are reached and service is affected.

### **1.1 Scope of the Plan**

This document represents the capacity plan for the key services supported by Agilisys over the twelve-month period starting in Jan 2019. As such, it considers the predicted future demands from users and balances them with the current utilisation of the various components of the service such as servers and network infrastructure in order to arrive at a recommended plan of action to ensure that service is maintained. It is intended to develop the tools and methods used during 2019 to allow more accurate recording of current usage and forecasting of future needs.

### **1.2 Methods Used**

Information concerning future usage of key services is collected as part of the regular IT service review process, and is a standard item on the agenda of each meeting. Service customers are asked to highlight any known increases or decreases in the usage of existing services and any other business events likely to impact on the effective provision of service.

Data regarding the current usage of technical resources is collected via a number of monitoring tools and is analysed at least quarterly to identify trends.

### **1.3 Assumptions Made**

In preparing this plan, the following assumptions have been made:

- Forecasts of future use are accurate, both in terms of timing and degree of change
- Measurements of current capacity usage are representative of typical demand

These assumptions will be reviewed on a regular basis to assess their continued validity.



## 2 Current and Forecast Demand for Services

There are several key business, technical, statutory, regulatory and contractual aspects that could potentially have an impact upon the capacity of the service in the timeframe under consideration.

### 2.1 Changes Affecting Capacity Requirements

The following changes are expected to have an impact on the capacity that needs to be provided over the next twelve months:

- Upgrade of the VDI solution to accommodate Office 365 and increasing user demand.
- Migration of users of Office Pro Plus and Office 365
- Migration of appropriate infrastructure to Microsoft Azure
- Various office moves
- Transition of Wigan CCG to the service
- Delivery of other ongoing Project deliverables

Each of these issues may have an impact not only on servers and networks but also on the support capacity within Agilisys.

### 2.2 Trends

In addition to these there are some general trends that will have an impact upon the available capacity. These are:

- The trend toward working from home by Partnership staff
- Increased volume of FAT devices across the Partnership
- Bring Your Own Device
- Increase in storage requirements for data backups due to retention
- Migration to Cloud based applications

These areas will be monitored over time to see how they develop.

### 3 Service and Resource Summary and Recommendations

The following table summarises the current capacity usage of the key components of Bolton and Wigan Partnership IT services, changes forecast over the current financial year, and recommendations for change made to ensure that sufficient capacity is provided to cope with the changes expected.

Resource	Description	Service(s)	Current Utilisation	Forecast	Recommendations	Priority
BWP Customer	VMWare ESX Environment	Infrastructure Hosting	CPU – Approaching Threshold	5% increase short-term due to CCG service	2 additional compute nodes purchased	High
BWP Customer	VMWare ESX Environment	Infrastructure Hosting	CPU – Approaching Threshold	25% reduction due to cloud migration	Remove older spec x3550 compute nodes (x4)	Low
V7000 (BaaS)	Backup Storage SAN	TSM and OVM Backup storage	89% - Approaching Warning Threshold	25% increase in space required	Purchase additional disk OR agree updated retention policies	High
WIG EXC	Wigan Exchange	Email	High	Reduction in required on-premise capacity	Reduction of 60% in on-premise capacity following migration	High
BOL EXC	Bolton Exchange	Email	Medium	Reduction in required on-premise capacity	Reduction of 50% in on-premise capacity following migration	Medium

Table 1 - Current capacity usage

### 3.1 Service Upgrades Required

The following service upgrades have been identified within the timeframe covered by this capacity plan.

Resource	Upgrade Required	Threshold	Timescale	Cost
BWP Customer	2x Compute Nodes (Already purchased)	.1 vCPU ratio to threshold	2 weeks to install	£24,000

*Table 2 - Service upgrades required*

### 3.2 Impact of New Technologies and New Techniques

Increasing use of Cloud based server virtualisation within BWP as a means of consolidating existing on premises servers onto fewer platforms and providing more flexibility in resource usage. This process will require a careful assessment of the capacity implications of doing this.

Cloud storage will have the effect of reducing our requirements for backup space and staff time in taking tapes offsite.

### 3.3 Other Recommendations

The following additional recommendations are made as a result of this review:

1. The upgrades listed in Table 2 should be procured to the timescales given
2. A review of tools required to manage and forecast Azure based services should be considered.
3. Consideration to be given to expanding toolset to improve monitoring of internet services regarding migration of services into cloud.



## Wigan Council Retention Schedule

### Places Directorate

Author: [REDACTED]

Date: 28 April 2016

## **Index**

Section 1 Consumer & Animal Protection

Section 2 Crime

Section 3 Economic Development

Section 4 Environmental Protection

Section 5 Planning and Building Control

Section 6 Transport and Highways

Section 7 Waste Management

Section 8 Skills and Employment

Section 9 Skills and Learning

Section 10 Greenspaces and Bereavement Services

Section 11 Housing Services

## Section 1 Consumer and Animal Protection

- 1.1 Adventure Activities
- 1.2 Animals and livestock
- 1.3 Complaints (*See Customer Service – General Support Functions Retention Schedule*)
- 1.4 Food
- 1.5 Health certificates
- 1.6 Incident Reports
- 1.7 Infectious Diseases
- 1.8 Licensing and registers (Excluding animals)
- 1.9 Lotteries
- 1.10 Motor salvage
- 1.11 Organic products
- 1.12 Pest Control
- 1.14 Premises
- 1.15 Product Safety
- 1.16 Prosecutions
- 1.17 Risk Assessments
- 1.19 Statutory Notices
- 1.20 Sunday Trading
- 1.21 Trading Standards
- 1.22 Water

## Consumer and Animal Protection

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
<b>1.1</b>	<b>Adventure Activities</b>				
1.1.1	Licence  Valid for no longer than 3 years	Whilst valid	To be in writing as prescribed in Regulation 8	Statutory	Adventure Activities Licensing Regulations 2004 SI 2004 No 1309 Regulations 3, 8 Revokes SI 1996/1309
1.1.2	Application for a licence	Until receipt of licence	To be a manner approved by the authority	Statutory	Adventure Activities Licensing Regulations 2004 SI 2004 No 1309 Regulation 4 Revokes SI 1996/1309
1.1.3	Register of licences  To be available for public inspection free of charge with copies available for free or for a reasonable charge	Recommend whilst valid plus 6 years	In a form considered appropriate by the licensing authority	Statutory	Adventure Activities Licensing Regulations 2004 SI 2004 No 1309 Regulation 13 Revokes SI 1996/1309
1.1.4	Annual Report	Recommend current year plus 3 years	None specified	Statutory	Adventure Activities Licensing Regulations 2004 SI 2004 No 1309 Regulation 18 Revokes SI 1996/1309
<b>1.2</b>	<b>Animals and Livestock</b>				
1.2.1	Animal Boarding	12 months after expiry of licence	None specified	Statutory	Animal Boarding Establishment Act 1963. Section 1 Licensing of boarding establishment for animals

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.2.2	Notices and licences	Recommend whilst valid + 12 months	Must be in writing	Statutory	Animal Gatherings (England) Order 2006 SI 2006 No 2211 Regulation 3  <b>Revokes SI 2004 No 1202</b>	
1.2.3	Animal trainers and exhibitors	12 months after expiry of licence	Paper (original)	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.2.4	Licences	Recommend two years from date of licence expires	To be carried (or a copy of it) at all times during the licensed movement	Statutory	Bluetongue Regulations 2008 SI 2008 No 962 Regulation 4  <b>Revokes SI 2007 No 3304 except for article 17.</b>	2.2.4
1.2.4.1	Consignment note	Recommend two years from date of consignment	To be carried at all times during the movement	Statutory	Bluetongue Regulations 2008 SI 2008 No 962 Regulation 4 (2)  <b>Revokes SI 2007 No 3304 except for article 17.</b>	2.2.4.1
1.2.4.2	Inventory of : Number of species dead Number alive that appear to have bluetongue Number alive that do not appear to have bluetongue.	To be kept up to date and held for at least two years	None specified	Statutory	Bluetongue Regulations 2008 SI 2008 No 962 Regulation 3  <b>Revokes SI 2007 No 3304 except for article 17.</b>	2.2.4.2
1.2.4.3	Export health certificate	Recommend 3 years from date of certificate	To be in writing	Statutory	Animals and Animal Products (Import and Export) (No 2) Regulations 2004 SI 2004 No 2886 Regulation 5 (1) (b)	



Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.2.4.4	Prohibition to export notice	Recommend 3years from date of notice	To be in writing Regulation 1 (3)	Statutory	Animals and Animal Products (Import and Export) (No 2) Regulations 2004 SI 2004 No 2886 Regulation 5 (2)	
1.2.4.5	Slaughter notice	Recommend 3 years from date of notice	To be in writing Regulation 1 (3)	Statutory	Animals and Animal Products (Import and Export) (No 2) Regulations 2004 SI 2004 No 2886 Regulation 5 (1) (b)	
1.2.4.6	Change of delivery address notice	Recommend 12 months from date of notification	To be in writing Regulation 1 (3)	Statutory	Animals and Animal Products (Import and Export) (No 2) Regulations 2004 SI 2004 No 2886 Regulation 7	
1.2.4.7	Dealers record of delivery of animals and their destination	12 months from arrival of the consignment	None specified	Statutory	Animals and Animal Products (Import and Export) (No 2) Regulations 2004 SI 2004 No 2886 Regulation 8	
1.2.4.8	Notification of anticipated date of arrival of consignment of animals	12 months from date of arrival	To be in writing	Statutory	Animals and Animal Products (Import and Export) (No 2) Regulations 2004 SI 2004 No 2886 Regulation 11	
1.2.4.9	Assembly centre register	Retain information for a minimum of 3 years	One specified	Statutory	Animals and Animal Products (Import and Export) (No 2) Regulations 2004 SI 2004 No 2886 Regulation 12 (4)	
1.2.4.10	Vehicle register Cattle, pigs, sheep and goats	To be preserved for 3 years	To be in writing	Statutory	Animals and Animal Products (Import and Export) (No 2) Regulations 2004 SI 2004 No 2886 Schedule 3 Part II - 2	
1.2.4.11	Record of import or export of cattle, pigs, sheep and goats by ID numbers or marks	To be preserved for 3 years	None specified	Statutory	Animals and Animal Products (Import and Export) (No 2) Regulations 2004 SI 2004 No 2886 Schedule 3 Part III - 4	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.2.5	Dangerous Wild Animals	12 months after expiry of licence	None specified	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.2.6	Dog breeding  Form in which record of breeding to be kept	12 months after expiry of licence	None specified	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1  Breeding of Dogs Act 1973 Section 1 (6)  The Breeding of Dogs (Licensing Records) Regulations 1999 SI 1999 No 3192 The Schedule	
1.2.7	Knackers' yards	12 months after expiry of licence	Paper (original)	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1  Animal By-product Regulations 2005 SI2005 No 2347	
1.2.8	Laying Hens - Register of establishments	Recommend whilst entry relevant plus 3 years	None specified	Statutory	Registration of Establishments (Laying Hens) (England) Regulations 2003 SI 2003 No 3100	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
1.2.9	Pet Shop and other establishments where animals are bred or kept for the purpose of carrying out business	12 months after expiry of licence	None specified	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1  By-laws  Pet Animal Act 1951 (Sections 2 and 3 repealed by the Animal Welfare Act 2006)  Animal Boarding Establishments Act 1964 and 1970  Breeding of Dogs Act 1973  Breeding and Sale of Dogs (Welfare) Act 1999
1.2.10	Pig movement	12 months after expiry of licence	Paper (original)	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1
1.2.11	Riding establishment licences	3 years after the last entry	None specified	Statutory	Riding Establishments Act 1964 Section 1 – Licensing of riding establishments
1.2.12	Zoos	12 months after expiry of licence	None specified	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.2.12.1	Directions made under the Zoo Licensing Act	6 years after the date of the direction	To be in writing	Statutory	Zoo Licensing Act 1981 (Amendment) England and Wales) Regulations 2002 SI 2002 No 3080 Regulation 25 (Inserts Section 19A into the Act)	
1.2.13	Holding Register	3 years from the end of the calendar year in which the last entry was made. Regulation 23 (9)	To be in writing	Statutory	Sheep and Goats (Records, Identification and Movement) (England) Order 2007 SI 2007 No 3493 Regulation 23 and Schedule 1  <b>Revokes SI 2005 No 3100 and SI 2006 No 2987</b>	
1.2.13.1	Movement document  Copy to be sent to local authority	3 years from the date of the movement of an animal on to his holding. Regulation 23 (2)	To be in writing	Statutory	Sheep and Goats (Records, Identification and Movement) (England) Order 2007 SI 2007 No 3493 Regulation 24 and Schedule 2  <b>Revokes SI 2005 No 3100 and SI 2006 No 2987</b>	
1.2.13.2	Annual inventory of animals	Recommend 3 years from 31 December each year	None specified	Statutory	Sheep and Goats (Records, Identification and Movement) (England) Order 2007 SI 2007 No 3493 Regulation 26  <b>Revokes SI 2005 No 3100 and SI 2006 No 2987</b>	
1.2.14	Notice of bovine animal at a show, exhibition, market, sale or fair being suspected of tuberculosis	Recommend 6 years from date of notice	To be in writing Regulation 20	Statutory	Tuberculosis (England) Order 2006. SI 2006 No 394 Regulation 16	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.2.15	Approvals, authorizations, licences and registrations	Recommend whilst relevant plus 3 years	Must be in writing	Statutory	Transmissible Spongiform Encephalopathies Regulations 2006 SI 2008 No 1881 Regulations 6, 15  <b>Revokes SI 2006 No 1228</b>	
1.2.16.1	The Food Standards Agency is the competent authority EXCEPT for butcher shops when it is the local authority.  See section 2.10.6	N/A	N/A	Statutory	Transmissible Spongiform Encephalopathies (No 2) (Amendment) Regulations 2007 SI 2007 No 1998  <b>Amends Schedule 6 of SI 2006 1228</b>	
1.2.16.1.1	Training records in slaughterhouse or cutting plant where specific risk material is removed	For as long as each person works there	None Specified	Statutory	Transmissible Spongiform Encephalopathies (No 2) (Amendment) Regulations 2008 SI 2008 No 1180  <b>Amends Schedule 6 of SI 2007 1998</b>	
1.2.17	Licences  Licence or copy to be carried during licensed movement	1 year from the date of the record	To be in writing	Statutory	Avian Influenza (Preventative Measures) (England) Regulations 2006 SI 2006 No 2701 Regulation 4	
1.2.18	Declarations, licences, notices and designations.  Licence or copy to be carried during licensed movement	Recommend period of declarations, licences, notices and designations. plus 3 years	Must be in writing	Statutory	Avian Influenza and Influenza of Avian Origin in Mammals (England) (No 2) Order 2006. SI 2006 No 2702 Regulation 4	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.2.18.1	Daily records of poultry, other captive birds and mammals	To be retained for at least 12 months from the date the record is made	None specified	Statutory	Avian Influenza and Influenza of Avian Origin in Mammals (England) (No 2) Order 2006. SI 2006 No 2702 Regulation 75. Schedule 1	
1.2.18.2	Record of visitors Record of poultry Record of poultry and egg movements	To be retained for at least 12 months from the date the record is made	None specified	Statutory	Avian Influenza and Influenza of Avian Origin in Mammals (England) (No 2) Order 2006. SI 2006 No 2702 Schedules 4, 5	
1.2.19	Declarations, licences, notices and designations.  Licence or copy to be carried during licensed movement	Recommend period of declarations, licences, notices and designations. plus 3 years	Must be in writing	Statutory	Avian Influenza (Vaccination) (England) Regulations 2006 SI 2006 No 2703 Regulation 4	
1.2.19.1	Records	To be retained for at least 12 months from the date the record is made	None specified	Statutory	Avian Influenza (Vaccination) (England) Regulations 2006 SI 2006 No 2703 Regulation 16	
1.2.20	Licences, notices and designations  Licence or copy to be carried during licensed movement	Recommend period of whilst relevant plus 3 years	Must be in writing	Statutory	Avian Influenza (H5N1 in poultry) (England) Order 2006 SI 2006 No 3247 Regulation 3	
1.2.20.1	Record of cleansing and disinfection of trolleys and trays to move eggs	12 months from the date the record is made  Regulation 18 (2)	None specified	Statutory	Avian Influenza (H5N1 in poultry) (England) Order 2006 SI 2006 No 3247 Regulation 10 (5) (c)	
1.2.20.2	Movement record	Retain for at least 6 weeks from the date the movement was completed	None specified	Statutory	Avian Influenza (H5N1 in poultry) (England) Order 2006 SI 2006 No 3247 Regulation 18	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.2.21	Declarations and notices	Recommend period of declarations and notices plus 3 years	Must be in writing	Statutory	The Avian Influenza (H5N1 in Wild Birds) (England) Order 2006 SI 2006 No 3249 Regulation 3	
1.2.21.1	Licences  Licence or copy to be carried during licensed movement	Recommend period of licence plus 3 years	Must be in writing	Statutory	The Avian Influenza (H5N1 in Wild Birds) (England) Order 2006 SI 2006 No 3249 Regulation 4	
1.2.21.2	Consignment note  To be carried at all times during licensed movement	6 weeks from date movement was completed  Regulation 15 (1) (b)	To be in writing	Statutory	The Avian Influenza (H5N1 in Wild Birds) (England) Order 2006 SI 2006 No 3249 Regulation 4 (6)	
1.2.21.3	Record Keeping <ul style="list-style-type: none"> <li>• What is moved, including quantity</li> <li>• Date of movement</li> <li>• Name of consignor</li> <li>• Address of premises from which movement started</li> <li>• Registration number of vehicle</li> <li>• Name of consignee</li> <li>• Address of destination</li> </ul>	6 weeks from date movement was completed  All other records to be retained for 12 months from the date the record is made.  Regulation 15 (2)	None stated	Statutory	The Avian Influenza (H5N1 in Wild Birds) (England) Order 2006 SI 2006 No 3249 Regulation 15	
1.2.22	Record of deliveries of animals and consignment notes	12 months from the arrival of the consignment	None specified	Statutory	Animals and Animal Products (Imports and Export) (England) Regulations 2006 SI 2006 No 1471 Regulation 8 (4)  <b>Revokes SI 2002 No 2002</b>	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.2.22.1	Certificates sent in accordance with these regulations	12 months from the date of arrival	None specified	Statutory	Animals and Animal Products (Imports and Export) (England) Regulations 2006 SI 2006 No 1471 Regulation 11 (2)  <b>Revokes SI 2002 No 2002</b>	
1.2.22.2	Assembly centre register	Each record in the register to be preserved for a minimum of 3 years	None specified	Statutory	Animals and Animal Products (Imports and Export) (England) Regulations 2006 SI 2006 No 1471 Regulation 12 (4) (b)  <b>Revokes SI 2002 No 2002</b>	
1.2.22.3	Vehicle register for the transport of Cattle, Pigs, Sheep and Goats	Preserve the information for 3 years	None specified	Statutory	Animals and Animal Products (Imports and Export) (England) Regulations 2006 SI 2006 No 1471 Schedule 3 Part II 2	
1.2.22.4	Record of all Cattle, Pigs, Sheep and Goats	Preserve the record for at least 3 years	None specified	Statutory	Animals and Animal Products (Imports and Export) (England) Regulations 2006 SI 2006 No 1471 Schedule 3 Part III 4	
1.2.22.5	Record of captive birds in quarantine	Retain for a least one year	None specified	Statutory	Animals and Animal Products (Imports and Export) (England) Regulations 2006 SI 2006 No 1471 Schedule 8 Part II 12	
1.2.23	Notification of hatcheries	Recommend two years from date of notification	None specified	Statutory	Poultry Breeding Flocks and Hatcheries (England) Order 2007 SI 2007 No 405 Regulation 4  <b>Revokes SI 1993 No 1898</b>	



Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.2.23.1	Notification of breeding flocks	Recommend two years from date of notification	None specified	Statutory	Poultry Breeding Flocks and Hatcheries (England) Order 2007 SI 2007 No 405 Regulation 5  <b>Revokes SI 1993 No 1898</b>	
1.2.23.2	Notification of arrival of breeding flocks	Recommend two years from date of notification	None specified	Statutory	Poultry Breeding Flocks and Hatcheries (England) Order 2007 SI 2007 No 405 Regulation 7  <b>Revokes SI 1993 No 1898</b>	
1.2.23.3	Notification of movement of laying phase etc	Recommend two years from date of notification	None specified	Statutory	Poultry Breeding Flocks and Hatcheries (England) Order 2007 SI 2007 No 405 Regulation 8  <b>Revokes SI 1993 No 1898</b>	
1.2.23.4	Records of samples	Two years from date sample was taken	None specified	Statutory	Poultry Breeding Flocks and Hatcheries (England) Order 2007 SI 2007 No 405 Regulation 11  <b>Revokes SI 1993 No 1898</b>	
1.2.23.5	Record of movements	Two years from date of movement	None specified	Statutory	Poultry Breeding Flocks and Hatcheries (England) Order 2007 SI 2007 No 405 Regulation 12  <b>Revokes SI 1993 No 1898</b>	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
1.2.23.6	Hatchery Records	Two years from date of movement	None specified	Statutory	Poultry Breeding Flocks and Hatcheries (England) Order 2007 SI 2007 No 405 Regulation 16  <b>Revokes SI 1993 No 1898</b>
1.2.24	An up to date register  Kept under Article 7 (1), first indent and Article 7 (4) of Regulation (EC) No 1760/2000.	10 years in the case of a farm and 3 years in any other case both from the end of the calendar year in which the last entry was made.  Any record made under the Bovine Animals (Records, Identification and Movement) Order must be kept for the same period	To be in writing Regulation 2 (2)	Statutory	Cattle Identification Regulations 2007. SI 2007 No 529 Regulation 5 and Schedule 5 Revokes <b>SI 1995 No 12</b> <b>SI 1998 No 871</b> <b>SI 1998 No 1796</b> <b>SI 1998 No 2969</b> <b>SI 1999 No 1939</b> <b>SI 2000 No 2976</b> <b>SI 2002 No 94</b> <b>SI 2002 No 95</b> <b>SI 2006 No 1538</b> <b>SI 2006 No 1539</b>
1.2.25	Notification of holdings		To be in writing Regulation 3	Statutory	Pigs (Records, Identification and Movement) Order 2007. SI 2007 No 642 Regulation 4  <b>Revokes SI 2003 No 2632</b>
1.2.25.1	Holding movement record Maximum number of pigs on holding	To be kept for at least 6 years	To be in writing Regulation 3	Statutory	Pigs (Records, Identification and Movement) Order 2007. SI 2007 No 642 Regulation 5  <b>Revokes SI 2003 No 2632</b>

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
1.2.25.2	Movement of pigs document (To be given to keeper at the destination)	To be kept for at least 6 months	To be in writing Regulation 3	Statutory	Pigs (Records, Identification and Movement) Order 2007. SI 2007 No 642 Regulation 12  <b>Revokes SI 2003 No 2632</b>
1.2.25.3	Walking licences for pigs	Must be carried during the walk	To be in writing Regulation 3	Statutory	Pigs (Records, Identification and Movement) Order 2007. SI 2007 No 642 Regulation 13  <b>Revokes SI 2003 No 2632</b>
1.2.26	Record of medicinal treatment Number of mortalities Welfare checks	Retain for a period of 3 years from the date medicinal treatment was given or the date of inspection	To be maintained. No specified format	Statutory	Welfare of farmed Animals (England) Regulation 2007 SI 2007 No 2078  Schedule 1 <b>Repeals SIs 2002/1870, 2002/1646, 2003/299 and Section 7 of the Agriculture (Miscellaneous Provisions) Act 1968.</b>
1.2.27	Seizure of stray dogs – register	12 months from date of entry	None specified	Statutory	Environmental Protection Act 1990 Section 149. Seizure of stray dogs. Register to be available for public inspection free of charge
1.2.28	Records in relation to exempt activities	To be kept for a period of at least two years	None stated	Statutory	Waste Management (England and Wales) Regulations 2006 SI 2006 No 937 Regulation 6  Amends the Waste Management Licensing Regulations 1994 SI 1994 No 1066

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
<b>1.3</b>	<b>Complaints – See Consumer Protection – General Support Functions Retention Schedule</b>					
<b>1.4</b>	<b>Food</b>					
1.4.1	Direction from the Food Standards Agency	6 years after direction is superseded or becomes invalid	Paper / electronic	Statutory	Food Standards Act 1999 Schedule 5	
1.4.2	GMO Proceedings not commenced within three years of the offence	3 years from date of offence.  No proceedings shall be commenced more than three years after the commission of the offence. Regulation 12 (2)	N/A	Statutory	Genetically Modified Organisms (Traceability and Labelling) (England) Regulations 2004. SI 2004 No 2412 Regulation 12 (2)	
1.4.3	Registers To be kept by the responsible authorities	Entries to be kept for not less than 3 years  Section 3 (5)	As specified in Section 3	Statutory	Environment and Safety Information Act 1988. 1988 Chapter 30 Section 3  The responsible bodies are those according to the Food and Environment Protection Act 1985 Section 19 (1)	
1.4.4	Notice (Food not to be used for human consumption)	Recommend 6 years from date the notice is withdrawn	To be in writing Section 49	Statutory	Food Safety Act 1990 1990 Chapter 16 Section 9	
1.4.4.1	Improvement notices	Recommend 6 years from date of improvement notice	To be in writing as prescribed in Sections 10 and 49	Statutory	Food Safety Act 1990 1990 Chapter 16 Section 10	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.4.4.2	Prohibition order	Recommend 6 years from the date the prohibition ceases to have effect	As imposed by the court	Statutory	Food Safety Act 1990 1990 Chapter 16 Section 11  Copies kept by the courts will fall under the record retention schedule approved by the Lord Chancellors Department and the Public Records Act	
1.4.4.3	Certification of end of prohibition order	Recommend 6 years from date of issue	To be in writing Section 49	Statutory	Food Safety Act 1990 1990 Chapter 16 Section 11 (7)	
1.4.5	Notice that sample will analyzed	6 years from date of notice	To be in writing	Statutory	Food Safety (Sampling and Qualifications) Regulations 1990 SI 1990 No 2463 Regulation 6 (3) (c), 8	
1.4.5.1	Certificate of analysis	6 years after date of certificate	To be in the form as set out in Schedule 3	Statutory	Food Safety (Sampling and Qualifications) Regulations 1990 SI 1990 No 2463 Regulation 9	
1.4.6	Application for registration Replaced by EC Regulation 852/2004	12 months after date of application	To be in writing as prescribed in Schedule 4	Statutory	Food Premises (Registration) Regulations 1991 SI 1991 No 2825 Regulation 4 Revoked by SI 2005 No 2059	
1.4.6.1	The register Replaced by EC Regulation 852/2004	Whilst valid	None specified but to contain the information prescribed in Regulation 5	Statutory	Food Premises (Registration) Regulations 1991 SI 1991 No 2825 Regulation 5  Revoked by SI 2005 No 2059	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.4.6.2	Supplementary record Replaced by EC Regulation 852/2004	None specified but to be separate from the register and contain the particulars required prescribed in Regulations 4 (4) or (5)	Whilst valid	Statutory	Food Premises (Registration) Regulations 1991 SI 1991 No 2825 Regulation 6 Revoked by SI 2005 No 2059	
1.4.7	Hygiene training and results	CY + 2 years	None specified	Corporate	Good business practice	
1.4.8	Registers	50 years after last entry	Paper / electronic	Statutory	Public Health Act 1936 Chapter 49	
1.4.10	Notice of removal or non use for failing to comply with Regulation 3	Recommend until revoked or withdrawn plus 6 years	To be in writing	Statutory	Bovine Products (Restrictions on Placing on the Market) (England) Regulations 2006. SI 2005 No 2719 Regulation 5	
1.4.11	Hygiene Improvement notices	Recommend date of notice plus 6 years	To be in writing Regulation 9	Statutory	Food Hygiene (England) Regulations 2006 SI 2006 No 14 Regulation 6	
1.4.11.1	Prohibition order	Recommend time expired or revoked plus 6 years	To be in writing Regulation 9	Statutory	Food Hygiene (England) Regulations 2006 SI 2006 No 14 Regulation 7	
1.4.11.2	Remedial action and detention notices	Recommend time expired, withdrawn or revoked plus 6 years	To be in writing Regulation 9	Statutory	Food Hygiene (England) Regulations 2006 SI 2006 No 14 Regulation 9	
1.4.11.3	Result of analysis or examination certificate	Recommend 6 years from date of certificate	To be in writing	Statutory	Food Hygiene (England) Regulations 2006 SI 2006 No 14 Regulation 13 (6)	
1.4.11.4	Documents held by food business operators	To be held for an appropriate period	None specified	Statutory	Community Regulations Article 5(4) (c) of Regulation 852/2006	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.4.11.5	Records showing number of birds and lagomorphs received into and fresh meat dispatched from producer	To be retained for one year	Records to be kept in adequate form	Statutory	Food Hygiene (England) Regulations 2006 SI 2006 No 14 Regulation 31 Schedule 5	
1.4.12	Laboratory tests	The operator shall keep a record of all results of all laboratory tests for at least two years  Regulation 32	To be in writing Regulations 3 and 20	Statutory	Animal By-products Regulations 2005 SI 2005 No 2347 Regulation 20	
1.4.12.1	Consigning, transporting or receiving animal by-products	To be kept for at least two years	To be in writing or electronic form	Statutory	Animal By-products Regulations 2005 SI 2005 No 2347 Regulation 33	
1.4.12.2	Burying or burning of animal by-products	To be kept for at least two years	To be in writing or electronic form	Statutory	Animal By-products Regulations 2005 SI 2005 No 2347 Regulation 34	
1.4.12.3	Disposal or use on premises of animal by-products	To be kept for at least two years	To be in writing or electronic form	Statutory	Animal By-products Regulations 2005 SI 2005 No 2347 Regulation 35	
1.4.12.4	Delivery records for biogas and composting plants	To be kept for at least two years	To be in writing or electronic form	Statutory	Animal By-products Regulations 2005 SI 2005 No 2347 Regulation 36	
1.4.12.5	Treatment records	To be kept for at least two years	To be in writing or electronic form	Statutory	Animal By-products Regulations 2005 SI 2005 No 2347 Regulation 37	
1.4.12.6	Records for approved laboratories	To be kept for at least two years	To be in writing or electronic form	Statutory	Animal By-products Regulations 2005 SI 2005 No 2347 Regulation 38	
1.4.12.7	Records of consignments of compost or digestion residue	To be kept for at least two years	To be in writing or electronic form	Statutory	Animal By-products Regulations 2005 SI 2005 No 2347 Regulation 39	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.4.12.8	Notice requiring the disposal of animal by-product or catering waste	To be kept for at least two years	To be in writing Regulation 3	Statutory	Animal By-products Regulations 2005 SI 2005 No 2347 Regulation 43	
1.4.12.9	Notice requiring cleansing and disinfection	To be kept for at least two years	To be in writing Regulation 3	Statutory	Animal By-products Regulations 2005 SI 2005 No 2347 Regulation 44	
1.4.12.10	Purchase and uses of photographic gelatine including disposal of residues and surplus materials	To be kept for at least two years	To be in writing Regulation 3	Statutory	Animal By-products Regulations 2005 SI 2005 No 2347 Regulation 51 (6)	
1.4.12.11	Processing or consigning of any ruminant animal by-products	To be kept for at least two years	To be in writing Regulation 3	Statutory	Animal By-products Regulations 2005 SI 2005 No 2347 Schedule 2 – 3 and 4	
1.4.13	Form of notification with a view to registration	Recommend whilst relevant plus 6 years	To be in writing	Statutory	Feed (Hygiene and Enforcement) (England) Regulations 2005 SI 2005 No 3280 Regulation 6	
1.4.13.1	Form of application for approval	Recommend whilst relevant plus 6 years	To be in writing	Statutory	Feed (Hygiene and Enforcement) (England) Regulations 2005 SI 2005 No 3280 Regulation 8	
1.4.13.2	Notice of suspension of registration or approval	Recommend whilst relevant plus 6 years	To be in writing Regulation 26	Statutory	Feed (Hygiene and Enforcement) (England) Regulations 2005 SI 2005 No 3280 Regulation 9	
1.4.13.3	Notice of revocation of registration or approval	Recommend whilst relevant plus 6 years	To be in writing Regulation 26	Statutory	Feed (Hygiene and Enforcement) (England) Regulations 2005 SI 2005 No 3280 Regulation 11	
1.4.13.4	Form of application for amendments to approval or registration.	Recommend whilst relevant plus 6 years	To be in writing	Statutory	Feed (Hygiene and Enforcement) (England) Regulations 2005 SI 2005 No 3280 Regulation 12	



Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.4.13.5	Improvement notices	Recommend whilst relevant plus 6 years	To be in writing Regulation 26	Statutory	Feed (Hygiene and Enforcement) (England) Regulations 2005 SI 2005 No 3280 Regulation 17	
1.4.13.6	Emergency Prohibition notices	Recommend whilst relevant plus 6 years	To be in writing Regulation 26	Statutory	Feed (Hygiene and Enforcement) (England) Regulations 2005 SI 2005 No 3280 Regulation 22	
1.4.13.7	Notice of inspection, seizure and detention of suspect feed	Recommend whilst relevant plus 6 years	To be in writing Regulation 26	Statutory	Feed (Hygiene and Enforcement) (England) Regulations 2005 SI 2005 No 3280 Regulation 25	
1.4.13.8	Improvement Notice	Recommend date of Notice plus 6 years	To be in writing Regulation 21	Statutory	Health & Safety at Work etc Act 1974 Section 21	
1.4.13.9	Prohibition Notice	Recommend date of Notice plus 6 years	To be in writing Regulation 22	Statutory	Health & Safety at Work etc Act 1974 Section 21	
1.4.13.10	Power to deal with cause of imminent danger (seizure)	Recommend date of Notice plus 6 years	To be in writing Regulation 25	Statutory	Health & Safety at Work etc Act 1974 Section 21	
<b>1.5</b>	<b>Health Certificates</b>					
1.5.1	Health certificates	CY + 5 years	Paper (Copy may be electronic)	Corporate	By-laws	
<b>1.6</b>	<b>Incident reports</b>					
1.6.1	Incident reports	CY + 6 years	None specified	Corporate	Good business practice	
<b>1.7</b>	<b>Infectious Diseases</b>					
1.7.1	Infectious disease reports	Archive	None specified	Corporate	Good business practice	
1.7.2	Cases of notifiable disease and food poisoning certificate	6 years from date of notification	paper	Statutory	Public Health (Control of Disease) Act 1984. Chapter 22. Section 11	
1.7.2.1	Certificate allowing child to return to school	6 years from date of 18 <sup>th</sup> birthday	paper	Statutory	Public Health (Control of Disease) Act 1984. Chapter 22. Section 21	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.7.2.2	List of school children at school having a case of notifiable disease	6 years from date of 18 <sup>th</sup> birthday	paper/electronic	Statutory	Public Health (Control of Disease) Act 1984. Chapter 22. Section 22	
1.7.2.3	Exclusion notice	6 years from date of notification	paper	Statutory	Public Health (Control of Disease) Act 1984. Chapter 22. Section 23	
1.7.2.4	Certificate to disinfect	6 years from date of notification	paper	Statutory	Public Health (Control of Disease) Act 1984. Chapter 22. Section 31	
1.7.2.5	Certificate of removal of person from infected house	6 years from date of notification	To be in writing (Section 58)	Statutory	Public Health (Control of Disease) Act 1984. Chapter 22. Section 32	
1.7.3	Notification to local authority of 'notifiable' devices	Life of devices plus 6 years	HSE approved form	Statutory	Notification of Cooling Towers and Evaporative Condensers Regulations 1992 SI 1992 No 2225 Regulation 3	

1.8	Licensing and registers ( Excluding animals)					
1.8.1	Applications	Validity of licence plus 1 year	None specified	Corporate	Good business practice Possibly offer to archivist	
1.8.2	Acupuncture, tattooing, ear piercing and electrolysis	12 months after expiry of licence	None specified	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.3	Advertisements – consent for display	12 months after expiry of licence	Paper (original)	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.5.0	Builders skips on highway	6 years	Paper	Statutory	Highways Act 1980 Section 139 and Section 55 of The Road Traffic Regulation Act 1967	
1.8.5.1	Pavement Café & Trade Displays	6 Years	Paper / Electronic	Statutory	Highways Act 1980 Section 115	

<b>Ref No</b>	<b>Title of Document [Local Name]</b>	<b>Retention Period</b>	<b>Current Format</b>	<b>Authority</b>	<b>Notes/Access</b>	
1.8.5.2	Oversailing license	6 Years following removal of the temporary structure	Paper / Electronic	Statutory	Highways Act 1980 Section 177	
1.8.5.3	Highway Projection	6 Years following removal of the structure	Paper / Electronic	Statutory	Highways Act 1980 Section 177	
1.8.7	Caravan Sites – Moveable dwellings	12 months after expiry of licence	None specified	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.10	Explosive licence Application	For as long as the licence or registration remains valid	To be in writing	Statutory	Manufacture and Storage of Explosive Regulations 2005 SI 2005 No 1082 Regulation 22	
1.8.10.1	Explosives – Health and safety representation in respect of an application	For as long as the licence or registration remains valid	To be in writing	Statutory	Manufacture and Storage of Explosive Regulations 2005 SI 2005 No 1082 Regulation 14	
1.8.10.2	Explosives licences	12 months after expiry of licence	To be in writing	Statutory	Manufacture and Storage of Explosive Regulations 2005 SI 2005 No 1082 Regulation 13	
1.8.10.3	Explosive licences – revoked To be returned to LA within 28 days	Recommend date of revocation + 6 years	To be in writing	Statutory	Manufacture and Storage of Explosive Regulations 2005 SI 2005 No 1082 Regulation 17	
1.8.10.4	Explosive licences – transfers	12 months after expiry of licence	To be in writing	Statutory	Manufacture and Storage of Explosive Regulations 2005 SI 2005 No 1082 Regulation 20	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.8.10.5	Explosives Register	Information on licence and application for as long as the licence or registration remains valid. Regulation 22	May be kept in any form including electronically	Statutory	Manufacture and Storage of Explosive Regulations 2005 SI 2005 No 1082 Schedule 4	
1.8.11	Explosives – Detonation resistance test certificate	2 years after the last disposal of relevant ammonia nitrate from the batch	None specified	Statutory	Ammonium Nitrate Materials (High Nitrogen Content) Safety Regulations 2003. SI 2003 No 1082 Regulation 3 (5)	
1.8.12	Gaming	12 months after expiry of licence	None specified	Statutory	Gambling Act 2005	
1.8.13	Hackney carriages and private hire vehicles. (Including drivers)	12 months after expiry of licence	None specified	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.14	Hairdresser's register	6 years from cessation of registration	None specified	Corporate		
1.8.15	Hypnotism	12 months after expiry of licence	Paper (original)	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.16	Loud speaker operation	12 months after expiry of licence	Paper (original)	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.17	Petroleum Spirit Licence	Whilst valid	Paper	Statutory	Petroleum Consolidation Act 1928 Sections 1 and 2 Petroleum spirit regulations 1929 SI 1929 No 992	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.8.18	Planting, retention and maintenance of trees in part of highway	12 months after expiry of licence	Paper (original)	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.19	Pleasure boats and pleasure vessels	12 months after expiry of licence	Paper (original)	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.20	Poisons - Persons entitled to sell non-medicinal poisons	12 months after expiry of licence	None specified	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.21	Poisons – sale of poisons	Whilst valid + 6 years	None specified	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.22	Poisons – register	Whilst valid + 6 years	None specified	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.23	Pool Betting - Annual statements of competitions	CY + 2 years	Paper	Statutory	Gambling Act 2005	
1.8.23.1	Pool promoters Track betting Inter – track betting schemes Amusement machines Amusement premises providing prizes	CY + 2 years	None specified	Statutory	Gambling Act 2005	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.8.24	Premises – Sale of Alcohol etc Premises Licence Personal Licence Temporary event licence Theatre Licence	Recommend whilst licence relevant + 6 years	To be in writing (Section 184 action suggests this)	Statutory	Licensing Act 2003 Chapter 17  <i>(There are in excess of 26 sections referring to records to be kept)</i>	
1.8.25	Premises for the preparation of food	Whilst valid + 6 years	Paper (original)	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.26	Scrap metal dealer	12 months after expiry of licence	None specified	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.27	Sex establishment	12 months after expiry of licence	None specified	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.28	Street traders	12 months after expiry of licence	None specified	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	
1.8.29	Street Works Licence (Section 50 New Roads and Street Works Act 1991)	12 months after expiry of licence	Paper and electronic	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.8.30	Window cleaners	12 months after expiry of licence	Paper Original)	Statutory	As authorised under The Local Authorities (Functions and Responsibilities) (England) Regulations 2000 SI 2000 No 2853 Schedule 1	

1.9	Lotteries					
1.9.1	A society's lottery return	2 years from date of return. At least 18 months for public inspection	None specified	Statutory	Gambling Act 2005	
1.9.1.1	Register of lotteries/raffles	2 years after last entry	None specified	Statutory	Gambling Act 2005	

1.10	Motor Salvage					
1.10.1	Register of motor salvage operators	To be kept up to date. Recommend 6 years from date of last active information	None specified	Statutory	Motor Salvage Operators Regulations 2002. SI 2002 No 1916 Data Protection Act 1998	

1.11	Organic Products. Imports from third countries					
1.11.1	Advanced notice for free circulation in the Community of the consignment	Recommend CY plus 3	To be in writing	Statutory	Organic Products Imports from Third Countries) regulations 2003. SI 2003 No 2821 Regulation 4	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
1.11.1.1	Notice to prohibit the movement of a consignment	Recommend CY plus 3	To be in writing	Statutory	Organic Products Imports from Third Countries) regulations 2003. SI 2003 No 2821 Regulation 5
1.11.1.2	Consent to movement	Recommend CY plus 3	To be in writing	Statutory	Organic Products Imports from Third Countries) regulations 2003. SI 2003 No 2821 Regulation 6

1.12	Pest Control				
1.12.1	Requests	CY + 2 years	None specified	Corporate	Pest Control

1.13	Premises				
1.13.1	Notices of hearings	6 years from date of determination or subsequent appeal	To be in writing Regulation 34	Statutory	Licensing Act 2003 (Hearings) Regulations 2005 SI 2005 No 44 Regulation 6
1.13.1.1	Reply to notice of hearing	6 years from date of determination or subsequent appeal	To be in writing Regulation 34	Statutory	Licensing Act 2003 (Hearings) Regulations 2005 SI 2005 No 44 Regulation 8
1.13.1.2	Hearing has been dispensed with	6 years from date of determination or subsequent appeal	To be in writing Regulation 34	Statutory	Licensing Act 2003 (Hearings) Regulations 2005 SI 2005 No 44 Regulation 9
1.13.1.3	Withdrawal of representations	6 years from date of determination or subsequent appeal	To be in writing Regulation 34	Statutory	Licensing Act 2003 (Hearings) Regulations 2005 SI 2005 No 44 Regulation 10
1.13.1.4	Information not given orally because of absence	6 years from date of determination or subsequent appeal	To be in writing	Statutory	Licensing Act 2003 (Hearings) Regulations 2005 SI 2005 No 44 Regulation 25



Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.13.1.5	Record of the proceedings	6 years from date of determination or subsequent appeal	None specified	Statutory	Licensing Act 2003 (Hearings) Regulations 2005 SI 2005 No 44 Regulation 30	
1.13.2	Enforcement	Date of completion + 6 years	None specified	Corporate	Good business practice	
1.13.3	Samples and analyses	CY + 6	None specified	Corporate	Limitation Act 1980	
1.13.4	Prescribed form for a temporary event	Date of event plus two years	To be in writing	Statutory	Licensing Act 2003 (Permitted Temporary Activities) (Notices) Regulations 2005 SI 2005 No 2918 Regulation 3 and Schedule 1	
1.13.4.1	Form of acknowledgment	Date of event plus 20 years	To be in writing	Statutory	Licensing Act 2003 (Permitted Temporary Activities) (Notices) Regulations 2005 SI 2005 No 2918 Regulation 4	
1.13.4.2	Counter notice	Date of event plus two years	To be in writing	Statutory	Licensing Act 2003 (Permitted Temporary Activities) (Notices) Regulations 2005 SI 2005 No 2918 Regulation 5 and Schedule 2	
1.13.4.3	Information and documents to accompany the notice of hearing.  Records of proceedings	6 years from the date that application or review is finally determined including any appeal or judicial review	To be in writing	Statutory	Gambling Act 2005 (Proceedings of Licensing Committees and Sub-committees) (Premises Licences and Provisional Statements) (England and Wales) Regulations 2007. SI 2007 No 173 Regulations 6 and 15	
1.13.5	Residential Premises Alarm Information	Until supersede	None Specified	Corporate	Good business practice	

<b>1.14</b>	<b>Product Safety</b>
-------------	-----------------------

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.14.1	Information on the risks of the product Documentation for tracing origin of product	Recommend life of product + 10 years	None specified	Statutory	The General Product Safety Regulations 2005. SI 2005 No 1803 Regulation 8	
1.14.1.1	Notification that product poses risks	Recommend life of product + 10 year	To be in writing	Statutory	The General Product Safety Regulations 2005. SI 2005 No 1803 Regulation 9	
1.14.1.3	Suspension Notice	Recommend life of product + 10 year	To be in writing	Statutory	The General Product Safety Regulations 2005. SI 2005 No 1803 Regulation 11	
1.14.1.4	Requirement to mark notice	Recommend life of product + 10 year	To be in writing	Statutory	The General Product Safety Regulations 2005. SI 2005 No 1803 Regulation 12	
1.14.1.5	Requirement to warn notice	Recommend life of product + 10 year	To be in writing	Statutory	The General Product Safety Regulations 2005. SI 2005 No 1803 Regulation 13	
1.14.1.6	Withdrawal notice	Recommend life of product + 10 year	To be in writing	Statutory	The General Product Safety Regulations 2005. SI 2005 No 1803 Regulation 14	
1.14.1.7	Recall Notice	Recommend life of product + 10 year	To be in writing	Statutory	The General Product Safety Regulations 2005. SI 2005 No 1803 Regulation 15	
1.14.1.8	Information to the public	Recommend life of product + 10 year	To be in writing	Statutory	The General Product Safety Regulations 2005. SI 2005 No 1803 Regulation 39	
1.14.2	Enforcement notices	Recommend date of notice plus 6 years	To be in writing	Statutory	Detergent Regulations 2005 SI 2005 No 2469 Regulation 9 (2)	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
1.14.2.1	Seizure and disposal notice	Recommend date of notice plus 6 years	To be in writing	Statutory	Detergent Regulations 2005 SI 2005 No 2469 Regulation 10 (5)	
1.14.3	Proceedings not commenced within 3 years of the offence	3 years from date of offence  No proceedings shall be commenced more than three years after the commission of the offence. Regulation 12 (2)	N/A	Statutory	Genetically Modified Organisms (Traceability and Labelling) (England) Regulations 2004 SI 2004 No 2412 Regulation 12 (2)	
<b>1.15</b>	<b>Prosecutions</b>					
1.15.1	Prosecutions	6 years after court case or significant action	None specified	Corporate	Limitation Act 1980 Possible offer to archivist	
<b>1.16</b>	<b>Risk Assessments See Health and Safety – General Support Functions Retention Schedule</b>					
<b>1.17</b>	<b>Statutory notices</b>					
1.17.1	Statutory notices	Whilst relevant plus 3 years	None specified	Corporate	Good business practice	
<b>1.18</b>	<b>Sunday Trading</b>					
1.18.1	Sunday Trading	1 year after entries have been deleted or superseded	None specified	Statutory	Sunday Trading Act 1994 Chapter 20 Schedule 1	
<b>1.19</b>	<b>Trading Standards</b>					
1.19.1	Inspection and Investigation visits	CY + 6 years	None specified	Corporate		

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
1.19.2	Instrument calibration <ul style="list-style-type: none"> <li>• Compliance notices</li> <li>• Immediate enforcement action</li> </ul>	Recommend CY + 6 years	Paper or electronic	Corporate	Measurement Instruments (Automatic Discontinuous Totalisers) Regulations 2006 SI 2006 No 1255 Regulation 18 and 19  See also SI 2006 No 1256 SI 2006 No 1257 SI 2006 No 1258 SI 2006 No 1259 SI2006 No 1264 SI 2006 No 1266 SI 2006 No 1267 SI 2006 No 1268 SI 2006 No 1269 SI 2006 No 1270
1.19.3	Statistical information	CY + 10 years	None specified	Corporate	Required for Dept of Trade and Office of Fair Trading
1.19.4	Trader enquiries	CY + 6 years	None specified	Corporate	
1.19.5	Prosecutions/ complaints/ trader files	6 years after business ceases trading	None specified	Corporate	

<b>1.20</b>	<b>Water</b>				
1.20.1	Test results of domestic / pool water	CY + 1 year	None specified	Corporate	

## **Section 2    Crime**

- 2.1            Anti social behaviour orders
- 2.2            Racial Incidents
- 2.3            Crime and Disorder Committee
- 2.4            CCTV
- 2.5            Violent Crime Reduction

## Crime

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
<b>2.1</b>	<b>Anti social orders</b>					
2.1.1	Parenting contracts	Recommend 3 years after contract ceases	None specified	Statutory	Police and Justice Act 2006 Chapter 48 Section 23  Amends Anti Social Behaviour Act 2003 Sections 3, 26	
2.1.2	Premise Closure Orders	Recommend 3 years after order ends	To be in writing	Corporate	Court Service destroys 3 years after the date the order was made	
2.1.3	Anti Social Behaviour Orders	Recommend 5 years after order ends	to be in writing	Statutory	Court Service destroys 5 years after the date the order expired	
<b>2.2</b>	<b>Racial incidents</b>					
2.2.1	Racial incident reports	5 years after last incident	None specified	Corporate		
<b>2.3</b>	<b>Crime and Disorder Committee</b>					
2.3.1	Reports and recommendations	Recommend 6 years after date of report or recommendation	None specified	Statutory	Police and Justice Act 2006 Chapter 48 Section 19	
2.3.2	Responses to considerations	Recommend 6 years after date of report or recommendation	None specified	Statutory	Police and Justice Act 2006 Chapter 48 Section 19	
<b>2.4</b>	<b>CCTV</b>					
2.4.1	CCTV Images	Retained for 31 days then overwritten by system unless required for evidential or intelligence purposes	Electronic	Corporate	Information required for evidential or intelligence purposes is archived off the live system . Retention is then decided by virtue of the matter concerned such as a prosecution for fly-tipping	

<b>Ref No</b>	<b>Title of Document [Local Name]</b>	<b>Retention Period</b>	<b>Current Format</b>	<b>Authority</b>	<b>Notes/Access</b>	
2.4.2	System Documentation: vetting and contractual information Technical Specifications etc	Permanent	None specified	Corporate	Information required to demonstrate the integrity of the system.	
<b>2.5</b>	<b>Violent crime reduction</b>					
2.5.1	Action Plan –Alcohol disorder Zone	Recommend whilst relevant plus 12 months	None specified	Statutory	Violent Crime Reduction Act 2006 Section 16 (4)	

## **Section 3 Economic Development**

- 3.1 European Social Fund [ESF]
- 3.2 European Regional Development Fund [ERDF]
- 3.3 NWDA Funding
- 3.4 Other Funders
- 3.5 Business Directory
- 3.6 Premises
- 3.7 Regeneration
- 3.8 National, Regional and Sub-Regional Development
- 3.9 Strategic files
- 3.10 Skills Funding Agency



## Economic Development

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
<b>3.1</b>	<b>European Social Fund [ESF]</b>					
3.1.1	Funding	CY plus 12 years	None specified	EU guidelines		
3.1.2	Data	Whilst relevant + 1 year	None specified	Corporate	Good business practice	
3.1.3	Reports	Closure of project + 12 years	None specified	Corporate	Good business practice Possibly offer to archivist	
<b>3.2</b>	<b>European Regional Development Fund [ERDF]</b>					
3.2.1	ERDF programme and project files	10 years from receipt of final payment	Original hard copies	Statutory	EU Obligation Legal requirement from funder	
<b>3.3</b>	<b>NWDA Funding</b>					
3.3.1	Regeneration SRB Coalfield Challenge Coalfields Programme	10 years from closure of programme	Original hard copies	Statutory	Legal requirement from funder	

<b>3.4</b>	<b>Other funders</b>					
3.4.1	Big Lottery	10 years from closure of programme	Original hard copies	Statutory	Legal requirement from funder	
3.4.2	Working Neighbourhoods Fund Area Based Grant	10 years from closure of programme	Original hard copies	Statutory	Legal requirement from funder	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
<b>3.5</b>	<b>Business Directory</b>					
3.5.1	Business Directory	Archive one copy	Electronic and CD Rom	Corporate	Common practice	

<b>3.6</b>	<b>Premises</b>					
3.6.1	Business enquiries on availability	CY + 2 years	None specified	Corporate	Common practice	
3.6.2	Premises / property register	Keep up to date	None specified	Corporate	Good business practice	
3.6.3	Newsletter	12 months	None specified	Corporate	Will the contents be of use to researchers in future years? If so consider scanning or microfilm	

<b>3.7</b>	<b>Regeneration</b>					
3.7.1	Buildings	Life of ownership + 16 years	None specified	Statutory	Limitation Act 1980	
3.7.2	Finance See Finance – General Support Functions Retention Schedule	CY + 6 years	None specified	Statutory	Audit Limitation Act 1980	
3.7.3	Publicity	CY + 2 years	None specified	Corporate	Good business practice – offer to archivist	

<b>3.8</b>	<b>National, Regional, Sub-Regional Development</b>					
3.8.1	Policy documents/strategies or plans	Drafts to be destroyed on approval of plan	Paper or electronic	Corporate	Good business practice	

<b>3.9</b>	<b>Strategic files</b>					
3.9.1	Strategic files	Until superseded then consider if important enough to archive	None specified	Corporate	Good business practice	

<b>3.10</b>	<b>Skills Funding Agency</b>					
3.10.1	Funding	CY plus 12 years	Hard copy/electronic	EU guidelines	Legal requirement from funder	
3.10.2	Data	Whilst relevant + 3 years	Hard copy/electronic	Corporate	Legal requirement from funder	
3.10.3	Reports	Closure of project + 12 years	None specified	Corporate	Legal requirement from funder	

## **Section 4      Environmental Protection**

- 4.1            Clean Air
- 4.2            Noise
- 4.3            Pollution (Including Fly Tipping)
- 4.4            Public registers

## Environmental Protection

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
<b>4.1</b>	<b>Clean Air</b>					
4.1.1	Notice of measurement of grit, dust and fumes by occupiers	Recommend 6 years from date of notice	To be in writing	Statutory	Clean Air Act 1993 Chapter 11 Section 10	
4.1.1.1	Records of measurement of grit, dust and fumes	Recommend 6 years from date of measurement	To be in writing	Statutory	Clean Air Act 1993 Chapter 11 Section 11	
4.1.1.2	Information about furnaces and fuel consumed	Recommend 6 years from date of information	To be in writing	Statutory	Clean Air Act 1993 Chapter 11 Section 12	
4.1.1.3	Notices requiring information about pollution	Recommend 6 years after date of supply of information. (The notice has a life of 12 months)	Issued notice to be writing	Statutory	Clean Air Act 1993 Chapter 11 Section 36	
4.1.1.4	Air Quality Review and Assessment	Until superseded then archive	None specified	Statutory	Environmental Act 1995 Section 83	
4.1.1.5	Air Quality Management and Areas	Until superseded then archive	None specified	Statutory	Environmental Act 1995 Section 84	
4.1.1.6	Air Quality Action Plan	Until superseded then archive	None specified	Statutory	Environmental Act 1995 Section 84	
<b>4.2</b>	<b>Noise</b>					
4.2.1	Noise level register	2 years from date of last entry in the register	None specified	Statutory	Control of Pollution Act 1974 Chapter 40 Section 64	
4.2.2	Noise abatement notice	6 years	None specified	Corporate	Environmental protection Act 1990 Section 80	
<b>4.3</b>	<b>Pollution</b>					
4.3.1	Training records Name of employee	"Must be kept for the required period"	None stated	Statutory	Ozone Depleting Substances (Qualifications) regulations 2006	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
	Training provided and date Date of issue of certificate(s)	Recommend employment plus 6 years			SI No 2006 No 1510 Regulation 7  Copy of record to be made available to employee if so requested	
4.3.2	Exempt waste operations – Record Keeping Register of exempt waste operations	To be kept for a period of 2 years	None stated	Statutory	Environment Permitting (England and Wales) Regulations 2007 SI 2007 No 3538 Regulation 12 (3)(b)	
4.3.3	Fly Tipping – Prosecution Files	CY + 6 Years	None stated	Corporate		

4.4	Public Registers					
4.4.1	Public registers	Permanent	As per schedule	Statutory	Environmental Permitting Regs 2007 SI 2007 No 3538 – Reg 46	
4.4.2	Contaminated Land	Permanent	As per schedule	Statutory	Environmental Protection Act 1990 Section 78R	
4.4.3	Radioactive substances	Permanent		Statutory	Radioactive Substances Act 1993 Section 39	

## **Section 5      Planning and Building Control**

- 5.1            Archaeological
- 5.2            Building Regulations
- 5.3            Conservation
- 5.4            Enforcement
- 5.5            Enquiries
- 5.6            Fees
- 5.7            Geographical Information System [GIS]/Mapping
- 5.8            Land drainage
- 5.9            Landscape
- 5.10          Listed buildings
- 5.11          Local Development Framework
- 5.12          Parks
- 5.13          Public Rights of Way
- 5.14          Planning applications
- 5.15          Policy
- 5.16          Roads – see Section 6, Transport and Highways
- 5.17          Structures
- 5.18          Trees
- 5.19          Brighter Borough (Transferred to Resources from 01/04/13)
- 5.20          Regeneration Projects and Grants
- 5.21          Sites of Biological Importance
- 5.22          Sites of Special Scientific Interest
- 5.23          Special Areas of Conservation
- 5.24          Local Nature Reserves

## Planning and Building Control

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
<b>5.1</b>	<b>Archaeological</b>				
5.1.1	Site files	Keep up to date. Review every 5 years	None specified	Corporate	Consider significant information for archives
<b>5.2</b>	<b>Building Regulations</b>				
5.2.1	Applications	10 years	Paper / electronic	Corporate	Consider significant information for archives
5.2.2	Building Control Approvals Certificate of completion	10 years from receipt	Paper / electronic (Latest applications determined must be kept for 3 years as paper copies)	Statutory	Building Act 1984 Section 56. Approved Inspectors Regulations 2000 Regulation 30 Building Control Performance Standard 7
5.2.3	Comments	CY + 3 years	None specified	Corporate	
5.2.4	Registers	Review every 15years	Paper / electronic	Corporate	Offer to archivist
5.2.5	Wigan Borough Demolition Files	1 year	Paper	Corporate	
<b>5.3</b>	<b>Conservation</b>				
5.3.1	Grants	6 years from completion of work or if EU 10 years from completion of work	None specified	Corporate	
5.3.2	Conservation Areas	Review every 5 years	Paper / electronic	Statutory	Planning (Listed Building & Conservation Areas) Act 1990
<b>5.4</b>	<b>Enforcement</b>				



Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
5.4.1	Inspections	12 years after issue of final certificate of inspection	Paper and electronic	Corporate		
5.4.2	Enforcement Notices/Stop Notices Breach of Condition Notices/Planning Contravention Notices	Permanent	Paper and electronic	Statutory	Town & Country Planning (development Management Procedure) (England) Order 2010 Part 7 Article 38	

5.5	Enquiries					
5.5.1	Enquiries / complaints / comments	CY + 2 years unless resulting in a significant change of policy. Then add to relevant file and consider archiving	None specified	Corporate		

5.6	Fees					
5.6.1	Fee structure	Current + 1 year	None specified	Corporate		
5.6.2	Receipts / accounts	CY + 6 years unless Audit authorises CY + 3 years	None specified	Audit		

5.7	Geographic Information System [GIS]/ Mapping					
5.7.1	Administrative boundaries – wards, parliamentary constituencies, borough boundaries (including meta data – information about information)	Keep indefinitely	Digital Paper	Corporate		
5.7.2	Contracts – see Finance - General Support Functions Retention Schedule					
5.7.3	Correspondence	CY plus 3 years	None specified	Corporate		

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
5.7.4	Aerial Photographs (including meta data)	Permanent	Digital Paper	Corporate	Keep for historical purposes  1984 and 1988 (hard copies, only partial coverage of Boro) 1997, 2000,2005, 2009 50% of Borough, 2011 50% of Borough (digital)
5.7.5	Metadata standards	Indefinitely	Electronic	Corporate	
5.7.7	Street Naming and numbering	Indefinitely for historical reference	Paper and electronic	Statutory	Town Improvement Clauses Act 1847 Public Health Act 1925 Greater Manchester Act 1981
5.7.8	Local Land and Property Gazetteer	Indefinitely for historical reference	Electronic	Statutory	Part of the street naming and numbering function created and maintained to British Standard 7666: 2006
5.7.9	National Street Gazetteer	Indefinitely for historical reference	Electronic	Statutory	Part of highway function under the New Roads and Street Works Act (1991)

5.8	Land drainage				
5.8.1	Sewer Records	Whilst relevant. Consult archives before disposal	Electronic	Corporate	
5.8.2	Land Drainage Records	Whilst relevant. Consult archives before disposal	Electronic	Corporate	
5.8.3	Drainage records	Whilst relevant. Consult archives before disposal	Electronic	Corporate	

5.9	Landscape				
5.9.1	Parish – Development Management	Development plus 16 years	None specified	Corporate	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
5.9.2	Landscape plans and drawings	5 years or as directed by funding body	Paper	Corporate		

5.10	Listed buildings					
5.10.1	Case file	Life of listed building plus 12 years. Consult archives before destruction	Paper / electronic	Statutory	Planning Listed Buildings & Conservation areas) Act 1990	

5.11	Local Plan					
5.11.1	Local development schemes	Recommend whilst current + 6 years	None specified	Statutory	Planning and Compulsory purchase Act 2004. Chapter 2004. Section 15	
5.11.1.1	Development Plan Documents	Recommend whilst current plus 6 years	None specified	Statutory	Planning and Compulsory Purchase Act 2004. Chapter 2004. Section 17	
5.11.1.2	Statement of community involvement	Recommend whilst current plus 6 years	None specified	Statutory	Planning and Compulsory Purchase Act 2004. Chapter 2004. Section 18	
5.11.1.3	Other Local Development plan documents	Recommend whilst current plus 6 years	None specified	Statutory	Planning and Compulsory Purchase Act 2004. Chapter 2004. Section 19	
5.11.1.4	Annual Monitoring Report	Recommend CY plus 6 years and then archive	None specified	Statutory	Planning and Compulsory Purchase Act 2004. Chapter 2004. Section 35	

5.12	Parks					
5.14.1	Historic parks and gardens	Review every 5 years and consult the archives before disposal	Paper	Corporate		

5.13	Public Rights of Way					
------	----------------------	--	--	--	--	--

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
5.15.1	Public Path Orders	Archive	Paper / electronic	Statutory	Town and Country Planning Act 1990	

5.14	Planning applications					
5.14.1	Case files – including: Planning applications Listed Building Consents Conservation Area Consents Prior Notifications Advertisement Consents High Hedges Licences Section 106 Agreements/Unilateral Undertakings Environmental Impact Assessments Environmental Impact Assessments – screening and scoping opinions	Indefinitely for records from 1945 where available. Planning Register (as set out in statute) has to be maintained.	Mix of paper and electronic files. Note – current files (Latest applications determined must be kept for 3 years as paper copies – Decision Notice, Application Form & Supporting Documents, Plans & Section 106 Documentation)	Statutory	Town & Country Planning (Development Management Procedure) (England) Order 2015, Part 9 Article 40	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
5.14.2	Appeal files – including: Forms Statements of Case Statement of Common Ground Proofs of Evidence Decision	Indefinitely for records from 1945 where available. Planning Register (as set out in statute) has to be maintained.	Paper and electronic	Statutory	Town & Country Planning (Development Management Procedure) (England) Order 2015, Part 9 Article 40

5.15	Policy				
5.15.1	Policy	Consider archiving significant changes in policy	None specified	Corporate	

5.16	Roads – see Section 6, Transport and Highways				
------	---	--	--	--	--

5.17	Structures				
5.17.1	Files	Life of structure plus 6 years	None specified	Corporate	
5.17.2	Inspections	CY + 6 years	None specified	Corporate	

5.18	Trees				
5.18.1	Tree Preservation Orders	Life of tree. Review every 5 years	Paper	Statutory	Town & Country Planning Act 1990 (The Tree Regulations 1999)

5.19	Brighter Borough (Transferred to Resources from 01/04/13)				
5.19.1	Application forms	11 years	Paper / electronic	Corporate	

5.20	Regeneration Projects and Grants				
------	----------------------------------	--	--	--	--

5.20.1	Project and Grant files	7 years from completion of work or if EU 10 years from completion of work	Paper/electronic	Corporate		
5.21	Sites of Biological Importance	For the life of the designation	Electronic	Corporate		
5.22	Sites of Special Scientific Interest	For the life of the designation	Paper and electronic	Statutory	Wildlife and Countryside Act 1981 CROW 2000	
5.23	Special Areas of Conservation	For the life of the designation	Paper and electronic	Statutory	Habitats Regulations 2010	
5.24	Local Nature Reserves	For the life of the designation	Electronic	Statutory	Nat. Parks etc. 1949	

## **Section 6    Transport and Highways**

- 6.1            Abnormal loads
- 6.2            Bridges
- 6.3            Car parks and parking
- 6.4            Crossings
- 6.5            Drainage
- 6.6            Highways
- 6.7            Reservoirs / lakes
- 6.8            Public right of ways
- 6.9            Street works
- 6.10          Works orders
- 6.11          Transport
- 6.12          Tunnels

## Transport and Highways

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
<b>6.1</b>	<b>Abnormal loads</b>				
6.1.1	Abnormal loads	Date of move plus 6 months unless regular load then weed annually	None specified	Corporate	
<b>6.2</b>	<b>Bridges</b>				
6.2.1	Assessment for HGV weight	Until superseded	None specified	Corporate	
6.2.2	Structure information	Life of bridge + 12 years but review and weed every 3 years	None specified	Corporate	May be required under the CDM regulations or other health and safety legislation
<b>6.3</b>	<b>Car parks and parking</b>				
6.3.1	Excess charge	CY + 6 years. Court cases - date of case + 6 years	None specified	Corporate	
6.3.2	Off and On street financial returns	CY + 2 years	None specified	Audit	
6.3.3	Parking permits	Expiry + 1 year	None specified	Corporate	<a href="#">view</a>
6.3.4.	Pay and display – audit tickets	CY + 6 years	Paper	Audit	Retaining indefinitely at present – possibility of reclaiming VAT - S
6.3.5	Pay and display – Test tickets	CY + 2 years	Paper	Audit	
6.3.6	Penalty charge notices [PCN's] - cancelled	CY + 2 years	Paper / electronic	Audit	
6.3.7	Penalty charge notices [PCN's] – copies	CY + 2 years	Electronic	Audit	
6.3.8	Penalty charge notices [PCN's] – paid	CY + 2 years	Electronic	Audit	
6.3.9	Penalty charge notices [PCN's] – representations	CY = 2 years	None specified	Corporate	Stored in Civica
6.3.10	Penalty charge notices [PCN's] – till rolls	CY + 6 years	Paper	Audit	



Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
6.3.11	Photographs	No dispute –28 days Settlement of dispute + 12 months	None specified	Corporate	These would be kept on the case itself and we retain case for 2+current.
6.3.12	Test tickets	CY + 3 years	Paper	Audit	APCOA hold the test tickets
6.3.13	Used car park tickets	1 year + CY	Paper	Audit	Retaining indefinitely at present – possibility of reclaiming VAT S [REDACTED]
6.3.14	Batches of payment receipts for fines Notices of offences (2 <sup>nd</sup> copy) – no requirement to keep 2 <sup>nd</sup> copy as electronic version on sidem DFES supporting documents	6 years + CY 3 years + CY 3 years + CY 6 years + CY	Paper	Audit	

6.4	Crossings				
6.4.1	Footpath applications	CY + 6 years	None specified	Corporate	
6.4.2	Rail	CY + 6 years	None specified	Corporate	
6.4.3	Road	CY + 6 years	None specified	Corporate	
6.4.4	School crossing location information	Keep up to date and archive periodically	Paper and electronic	Corporate	In accordance with national guidelines for service delivery

6.5	Drainage				
6.5.1	Gully emptying schedules	Review annually	Paper / electronic	Corporate	
6.5.2	Historical records	Permanent	Paper / electronic	Corporate	Information Placed on GIS
6.5.3	Management and maintenance	Review annually. Retain essential information for the life of the drainage system	None specified	Corporate	May be required under the CDM regulations or other health and safety legislation

6.6	Highways				
Note	For Highway maintenance refer to the	Quote	Electronic	Corporate	Code of Practice for Maintenance

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
	publication in column 6 which states that comprehensive and accurate records should be kept of all highway maintenance activities and in particular <ul style="list-style-type: none"> <li>• Safety Inspections</li> <li>• Other inspections</li> <li>• Identifying the time of any response</li> <li>• Identifying the nature of any response (including nil returns)</li> <li>• Subsequent follow up action</li> </ul>	“Arrangements should be established to ensure effective co-ordination of all highway maintenance records with other relevant record systems, including road accident information, together with a programme for regular review” End of quote Review every 5 years and weed as necessary			Management (Delivering Best Value in Highway Maintenance) available from the Institute of Highways	
6.6.1	Section 38 Agreements Section 278 Agreements	Job file CY + 6 years  Detailed plans indefinitely	Paper and electronic  Paper and electronic	Corporate  Corporate	Actual signed Agreement held by Legal indefinitely	
	Highway Design Contracts (under seal) Highway Design Contracts (under hand)	12 years 6 years		Statutory Statutory	Legal requirement Legal Requirement	
6.6.2	Budgets	CY + 3 years	None specified	Audit		
6.6.3	Contracts – see Finance – General Support Functions Retention Schedule					
6.6.4	Defects				CY + 2 years	None specified Corporate
6.6.5	Licences	Life of licence + 1 year	None specified	Corporate		
6.6.6	Highway Adoption Register	To be maintained	Must be kept in	Statutory	Dedicated Highways (Registers under	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
		and archived periodically	both electronic and paper form		Section 31A of the Highways Act 1980) SI 2007 No 2334
6.6.7	Obstruction removal. Forms 1 – 5 as described in the Schedule	Recommend date of issue + 6 years	To be in writing	Statutory	Removal of Obstructions From Highways (Notices etc) (England) regulations 2004. I 2004 No 370 Regulation 2
6.6.8	Permanent road closures	To be maintained and archived periodically	Electronic and Paper	Corporate	
6.6.9	Temporary road closures	To be maintained and archived periodically	Electronic and Paper	Corporate	
6.6.10	Road accidents	To be maintained and archived periodically	Electronic	Corporate	This is TfGM data which they share with us. We just have access it is not our data.
6.6.11	Schemes	5 years before being archived	Electronic	Corporate	LTP Schemes - Stored electronically
6.6.12	Traffic Orders	To be maintained and archived periodically	Paper and electronic	Corporate	
6.6.13	Road Safety Audits	To be maintained and archived periodically	Paper	Statutory	Legal Requirement as per our Safety Audit Policy
6.6.14	Integrated Transport Unit - BSOG	12mths after grant awarded	Paper	Statutory	
6.6.15	Integrated Transport Unit - Staff Personal Files	Three years	Paper	Corporate	Associated with operational workforce

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
<b>6.7</b>	<b>Reservoirs / lakes</b>					
6.7.1	Reservoirs / lakes	Review every 25 years Consult Local history Officer or Archivist	None specified	Statutory	Reservoirs Act 1975 SI 1985 No 548	
<b>6.8</b>	<b>Public rights of ways</b>					
6.8.1	Access schemes – Rights of Way Improvement Plan	Review at closure. If of significant interest then assess and archive	Paper and electronic	Statutory	Countryside and Rights of Way Act 2000	
6.8.2	Consultation and notification lists	CY + 2 years	Paper and electronic	Corporate		
6.8.3	Definitive map	Keep up to date	Paper and electronic	Statutory	Wildlife and Countryside Act 1981	
6.8.4	Definitive map modification [DMMO's]	Archive	Paper	Statutory	Wildlife and Countryside Act 1981	
6.8.5	Maintenance schedules and inspections	Until superseded	Paper and electronic	Statutory	Highways Act 1990 and Inspection Policy	
6.8.6	Maintenance works orders	Assess every 5 years and archive	Paper and electronic	Statutory	Highways act 1980 and Inspection Policy	
6.8.7	Public Path Orders [PPO's]	Archive	Paper	Statutory	Highways Act 1980	
6.8.8	Register of applications under Section 53 (5) of the Wildlife and Countryside Act	To be updated as soon as reasonably practicable	Electronic and paper form. A website version to be publicly available	Statutory	Public Rights of Way (Register of Applications under section 53 (5) of the Wildlife and Countryside Act 1981) (England) Regulations 2005 SI 2005 No 2461	
6.8.9	Register of Highway Statements and Declarations Highways Act 1980 Section 31(6)	To be updated as soon as reasonably practicable	Electronic and paper form. A website version to be publicly available	Statutory	Register of Highway Act Declarations, Statements and Maps (England) SI 2334	
6.8.10	Register of exclusions of the right to apply under Section 15(1) to register new	To be updated as soon as reasonably	Electronic and paper form. A	Statutory	Deposits made under Section 15A(1) of the Commons Act 2006	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
	town or village green	practicable	website version to be publicly available		
6.8.11	Removal of obstructions/enforcement	To be assessed every 5 years and archived	Paper	Statutory	Highways Act 1980

<b>6.9</b>		<b>Street works</b>				
6.9.1	NRSWA footways and highways maintenance	CY + 6 years	Electronic	Statutory	Roads and Street Works Act	
6.9.2	Register of utilities	Keep up to date	Electronic	Corporate		
6.9.3	Register	Keep up to date	None specified	Statutory	Street Works (Registers, Notices, Directions and Designations) (England) Regulations 2007  SI 2007 No. 1951	
6.9.4	Register of permits	<b>Access to register</b>  34.—(1) The Permit Authority shall make the register available for inspection, at all reasonable hours and free of charge	None specified	Statutory	Traffic Management Permit Scheme (England) Regulations 2007 SI 2007 No 3372 Regulation 33	
6.9.5	Street lighting scheme details	CY + 6	Electronic	Corporate	Inventory records maintained for street lighting equipment currently operating	
6.9.6	Street lighting inspection and testing	CY + 6	Electronic	Corporate		

<b>6.10</b>		<b>Works orders</b>				
6.10.1	Monitoring	6 or 12 years after	None specified	Corporate	Good business practice	

		contract finishes – see Finance – General Support Functions Retention Schedule				
<b>6.11</b>	<b>Transport</b>					
6.11.1	Vehicle Documentation MOT Records Vehicle Inspection History	Ownership of vehicle plus 6 yrs (For council vehicles) Or 6 years from date of inspection for other vehicles	Electronic	Corporate		
	<b>Leigh Building Services</b>					
6.11.2	Waste Transfer Station Documentation Site Diary Incoming and Outgoing Waste Amounts Waste Consignment Notes	2 years	Paper	Statutory	Environmental Protect Act 1990	
6.11.3	LOLA Tests	1 year	Paper	Statutory	Operations and Lifting Equipment Regulations 1998	
6.11.4	Pressure vessel tests	1 year	Paper	Statutory	Pressure Equipment Regulations 1999	
6.11.5	Weighbridge maintenance and calibration	1 year	Paper		Good practice	
<b>6.12</b>	<b>Tunnels</b>					
6.12.1	Designation of administration authority	Until superseded	To be in writing	Statutory	Road Tunnel Safety Regulations 2007 SI 2007 No 1520 Regulation 4 (4) (a)	
6.12.1.1	Operational and organizational schemes	Whilst relevant	To be writing	Statutory	Road Tunnel Safety Regulations 2007 SI 2007 No 1520 Regulation 5 (3)	
6.12.1.2	Accident and fire reports		None specified	Statutory	Road Tunnel Safety Regulations 2007 SI 2007 No 1520 Regulation 6	

6.12.1.3	Inspections and reports	Recommend 6 years from the date made	None specified	Statutory	Road Tunnel Safety Regulations 2007 SI 2007 No 1520 Regulation13	
6.12.1.4	Risk analysis	Until superseded	None specified	Statutory	Road Tunnel Safety Regulations 2007 SI 2007 No 1520 Regulation 18	
6.12.1.5	Request for a derogation	Recommend life of the tunnel	To be in writing	Statutory	Road Tunnel Safety Regulations 2007 SI 2007 No 1520 Regulation 19	

## **Section 7 Waste Management**

- 7.1 Property and waste collection
- 7.2 Public Register
- 7.3 Service Monitoring
- 7.4 Trade Refuse
- 7.5 Waste



## Waste Management

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access	
<b>7.1</b>	<b>Property and waste collection</b>					
7.1.1	Requested collections	Date of collection + 6 months	None specified	Corporate		
7.1.2	Collection reports: Data Preparation Stats Reports Weekly Summaries Incident Reports	CY + 2 years	None specified	Corporate		
<b>7.2</b>	<b>Public Register</b>					
7.2.1	Public registers	A regulator is not required to keep in its public register information which is no longer relevant for the purposes of public participation required under these regulations	May be kept in any form	Statutory	Environmental Protection Act 1990 Chapter 43 as amended the Environment Act 1995 Chapter 25  As amended by Environment Permitting (England and Wales) Regulations 2007 SI 2007 No 3538  Possibly offer to archivist	
<b>7.3</b>	<b>Service monitoring</b>					
7.3.1	Service monitoring	CY + 6 years	None specified	Corporate	Good business practice	
<b>7.4</b>	<b>Trade refuse</b>					
7.4.1	Household Waste Recycling Centre Access Permits	5 years from date of issue	None specified	Corporate		
<b>7.5</b>	<b>Waste</b>					
7.5.1	Notices, notifications, returns	2 years beginning on the day after the day on which the	To be in writing	Statutory	Landfill Allowances and Trading Scheme (England) Regulations 2004	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
		reconciliation period for the scheme year ends Regulation 11 (4) and 12 (3)			SI 2004 No 3212 Regulation 3
7.5.1.2	Registers	To be available for inspection free of charge with copies at a reasonable charge.	May be in an electronic format	Statutory	Landfill Allowances and Trading Scheme (England) Regulations 2004  SI 2004 No 3212 Regulation 4  Possibly offer to archivist
7.5.2	Waste tonnage	CY + 6 years	None specified	Corporate	Good business practice
7.5.3	Waste transfer notes	CY+ 2 years	Paper	Statutory	Environmental Protection (Duty of Care) Regulations. 1991 SI 1991 No 2839  NB. The waste management contractor must retain notes for 6 years under landfill tax legislation.
7.5.3.1	Declaration of compliance	Recommend whilst relevant plus 6 years	To be in writing Electronic formats may be used Regulation 2(2)	Statutory	Waste Electrical and Electronic Equipment Regulations 2006 SI 2006 No 3289 Regulations 12, 29
7.5.3.2	Record Keeping <ul style="list-style-type: none"> <li>The amount of tonnes of all EEE he has put on the market in the UK in a compliance period by categories.</li> <li>The amount of tonnes collected or delivered</li> <li>Number units returned from private households</li> </ul>	4 years from date on which the record is made	May be electronic	Statutory	Waste Electrical and Electronic Equipment Regulations 2006 SI 2006 No 3289 Regulations 13, 30, 34, 53

<b>Ref No</b>	<b>Title of Document [Local Name]</b>	<b>Retention Period</b>	<b>Current Format</b>	<b>Authority</b>	<b>Notes/Access</b>	
7.5.3.3	Information on new types of EEE	Recommend 10 years after the last item has been dispatched	May be electronic	Statutory	Waste Electrical and Electronic Equipment Regulations 2006 SI 2006 No 3289 Regulation 17	
7.5.3.4	Notification of new scheme members	Recommend 6 years after they cease to be come members	To be in writing	Statutory	Waste Electrical and Electronic Equipment Regulations 2006 SI 2006 No 3289 Regulation 21	
7.5.3.5	Preliminary and final notification specifying WEEE for which operator is responsible for.	Recommend 6 years from date of notice	To be in writing	Statutory	Waste Electrical and Electronic Equipment Regulations 2006 SI 2006 No 3289 Regulation 22 (4)	
7.5.3.6	Reports on collection and disposal totals	Recommend 4 years from date of report	To be in writing	Statutory	Waste Electrical and Electronic Equipment Regulations 2006 SI 2006 No 3289 Regulation 27	
7.5.3.7	Reports of EEE put on the market	Recommend 4 years from date of report	To be in writing	Statutory	Waste Electrical and Electronic Equipment Regulations 2006 SI 2006 No 3289 Regulation 28	
7.5.3.8	Register of producers Open to the public	Superseded information may be discarded after the later information has been entered for 4 years	In any format but must be indexed	Statutory	Waste Electrical and Electronic Equipment Regulations 2006 SI 2006 No 3289 Regulation 60	

## Section 8 Employment and Skills

8.1	National Careers Service Contract Documents, Action Plans and Paid outcomes	Records to be kept for 10 years after completion of programme	Original documentation	Statutory	Condition of contract
8.2	Supported Employment Service User information where the referral source is non - DWP	Records to be kept 7 years from date of closure	Hard copies now back scanned saved as electronic files - civica	Corporate Guidelines – from historic position with Adult Services	Closed hard files previously sent to Iron Mountain with instruction to destroy in 7 years.
8.3	Supported Employment Service User information where the referral source is non - DWP	Records to be kept 7 years from date of closure	Electronic Files (word, excel & Asset)	Corporate Guidelines	Still in existence on G:drive.
8.4	Supported Employment – Workchoice Referrals	31st December 2022	Original Hard Copies Electronic Files (word, excel, Asset & STEP)	DWP Guidelines and EU Guidelines	<p>Work Choice Participant records are transferred to Shaw Trust for archiving either at the end of the Work Choice programme or earlier termination of your Work Choice Sub-contract.</p> <p>OR</p> <p>Participant records are retained by you in a secure environment for as long as is required after the Work Choice programme ends under Work Choice document retention rules.</p>

8.5	Supported Employment – Specialist Employment Support	At least 31 <sup>st</sup> December 2023.	Original Hard Copies - currently stored securely on site.  Electronic copies – scanned docs on G:Drive	DWP Guidelines and EU Guidelines	The Provider shall maintain the records 1 and such other documents as may reasonably be required throughout the Contract Period and shall retain such records and documents until at least 31 <sup>st</sup> December 2023.
-----	--	--	--	----------------------------------	--

## **Section 9 Skills and Learning**

- 9.1 Skills Funding Agency 16-18 Apprenticeships and Traineeships
- 9.2 Skills Funding Agency Adult Skills Budget and 19+ Traineeships
- 9.3 Skills Funding agency Community Learning
- 9.4 Management Information Returns Sub Contractor Documentation

## Section 9 Skills and Learning

9.1	<b>Skills Funding Agency 16-18 Apprenticeships and Traineeships</b>				
9.1.1	Enrolment Forms/ Learner Agreements	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract
9.1.2	Assessment Documentation/ Learner Support	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract
9.1.3	Registers of Attendance	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract
9.1.4	Individual Learning Plans	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract
9.1.5	Progress Reports	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract
9.1.6	Learner Declaration Forms	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract

9.1.7	Evidence of Achievement	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Copies of Certification	Statutory	Condition of Contract
	The Council and it's sub-contractors to retain original invoices; management information returns and all other documents necessary to verify the provision delivered by itself or by its sub-contractors	6 years from the end of the financial year in which the last payment is made.	Original documentation	Statutory	Condition of contract
9.2	<b>Skills Funding Agency Adult Skills Budget and 19+ Traineeships</b>				
9.2.1	Enrolment Forms/ Learner Agreements	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract
9.2.2	Assessment Documentation/ Learner Support	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract
9.2.3	Registers of Attendance	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract
9.2.4	Individual Learning Plans	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract



9.2.5	Progress Reports	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract
9.2.6	Learner Declaration Forms	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract
9.2.7	Evidence of Achievement	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Copies of Certification	Statutory	Condition of Contract
<b>9.3</b>	<b>Skills Funding Agency Community Learning</b>				
9.3.1	Enrolment Forms/ Learner Agreements	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract
9.3.2	Registers of Attendance	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract
9.3.3	Individual Learning Plans	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Must contain authentic signatures	Statutory	Condition of Contract

9.3.4	Evidence of Achievement	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation. Evidence of Learning taken place	Statutory	Condition of Contract
<b>9.4</b>	<b>Management Information Returns and the Council's Sub Contractor Invoices and documentation necessary for proof of provision delivered</b>				
9.4.1	Electronic / Paper based Individual Learner Records	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation.	Statutory	Condition of Contract
9.4.2	Sub Contractor Declaration Information	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation.	Statutory	Condition of Contract
9.4.3	Annual Fees and Charging Policy	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation.	Statutory	Condition of Contract
9.4.4	Contracts and Service Level Agreements	6 years from the year in which learning took place. If ESF match funded 12 years	Original/electronic documentation.	Statutory	Condition of Contract

## Section 10 – Greenspaces and Bereavement Services

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
<b>10.1</b>	<b>Bereavement Services - Cremation</b>				
10.1.1	Form H – Particulars for Cremation	15 years	Original paper format – completed as part of the process	Statutory	Records kept within the local office for 5 years after which time they are transferred to Leigh walk in safe for temporary archiving prior to shredding after 15 year period
10.1.2	Application for the cremation of a body of a person who has died (Family Form) – (Cremation 1)	15 years	Original paper format – completed as part of the process	Statutory	Records kept within the local office for 5 years after which time they are transferred to Leigh walk in safe for temporary archiving prior to shredding after 15 year period
10.1.3	Cremation Medical Certificate – (Cremation 4)	15 years	Original paper format – completed as part of the process	Statutory	Records kept within the local office for 5 years after which time they are transferred to Leigh walk in safe for temporary archiving prior to shredding after 15 year period
10.1.4	Confirmatory Medical Certificate (Cremation 5)	15 years	Original paper format – completed as part of the process	Statutory	Records kept within the local office for 5 years after which time they are transferred to Leigh walk in safe for temporary archiving prior to shredding after 15 year period
10.1.5	Cremation Authorisation of cremation of deceased person by Medical Referee (Cremation 10)	15 years	Original paper format – completed as part of the process	Statutory	Records kept within the local office for 5 years after which time they are transferred to Leigh walk in safe for temporary archiving prior to shredding after 15 year period
<b>10.1.6</b>	Certificate of Coroner (Cremation 6)	15 years	Original paper format –	Statutory	Issued by Coroner Records kept within the local office for 5

			completed as part of the process		years after which time they are transferred to Leigh walk in safe for temporary archiving prior to shredding after 15 year period
10.1.7	Certificate for Burial or Cremation – Part B	15 years	Original paper format – completed as part of the process	Statutory	Issued by Registrar of Births Deaths and Marriages Records kept within the local office for 5 years after which time they are transferred to Leigh walk in safe for temporary archiving prior to shredding after 15 year period
<b>10.2</b>	<b>Bereavement Services Burial</b>				
10.2.1	Notice of Interment	10 years	Original paper format – completed as part of the process	Ministry of Justice guidelines	Records kept within the local office for 5 years after which time they are transferred to Leigh walk in safe for temporary archiving prior to shredding after 10 year period
10.2.2	Form of Indemnity – (in absence of Original Grave Deed)	10 years	Original paper format – completed as part of the process	Local Authority Guidelines	To protect the LA against all claims action. Damages from the opening of a council grave. From October 2015 – indemnity forms no longer used as legal process now followed
	Certificate for Burial or Cremation – Part B	10 years		Statutory	Issued by Registrar of Births Deaths and Marriages Records kept within the local office for 5 years after which time they are transferred to Leigh walk in safe for temporary archiving prior to shredding after 10 year period
<b>10.3</b>	<b>Bereavement Services - Memorialisation</b>				
10.3.1	New Memorial Application (Headstone)	10 Years	Original paper format – completed as part of the process From April 2016	Corporate	Records kept within the local office for 5 years after which time they are transferred to Leigh walk in safe for temporary archiving prior to shredding after 10 year period, this forms the basis of the Memorial Mason Guarantee.

			applications scanned once local checks undertaken.		
10.3.2	Application to carry out additional inscriptions to an existing memorial	10 Years	Original paper format – completed as part of the process From April 2016 applications scanned once local checks undertaken.	Corporate	Records kept within the local office for 5 years after which time they are transferred to Leigh walk in safe for temporary archiving prior to shredding after 10 year period, this forms the basis of the Memorial Mason Guarantee.
10.3.3	Application for a memorial tablet for cremated remains	10 Years  Once scanned no paper retention.	Original paper format – completed as part of the process From April 2016 applications scanned once local checks undertaken.	Corporate	Records kept within the local office for 5 years after which time they are transferred to Leigh walk in safe for temporary archiving prior to shredding after 10 year period, this forms the basis of the Memorial Mason Guarantee.
10.3.4	Columbarium Application Form	7 Years  Once scanned no paper retention.	Original paper format – completed as part of the process New product all applications can be scanned and attached to the grave record.	Corporate	Acceptance of rules and regulations
10.3.5	Barbican Memorial Tablet Application Form	0 Years  Once scanned no	Original paper format – completed as	Corporate	Acceptance of rules and regulations

		paper retention	part of the process New product all applications can be scanned and attached to the grave record.		
10.3.6	Memorial Leaf Application Form	0 Years  Once scanned no paper retention.	Original paper format – completed as part of the process New product all applications can be scanned and attached to the memorial record.	Corporate	Contact Information
10.3.7	Book of Remembrance Application Form	30 Years	Original paper format – completed as part of the process All applications currently stored in paper format process needed to digitise.	Corporate	

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
<b>10.4</b>	<b>Greenspace Services –Play</b>				
10.4.1	Parks and open spaces – Site inspection records	CY + 6 years	Paper	Corporate	

10.4.2	Play Site Inspection – Weekly Visual Inspection and 3 Monthly Operational Inspection	21 years	Paper and Electronic PDF Files	Statutory	
10.4.3	ROSPA - Bi-Annual	21 years	Paper and electronic	Statutory	
10.4.4	ROSPA post installation	21 Years	Paper and electronic	Statutory	
10.4.5	Insurance claim file		Paper and electronic	Corporate	A mixture of various response requirements / photographs etc.; Local file – main file kept with insurance section
10.4.6	Site development - suppliers plans and documents	6 years	Paper and electronic		
<b>10.5</b>	<b>Greenspace Services –Parks Management and Development</b>				
10.5.1	Event Application Form and submission requirements (Risk Assessment, Licences , Performing Rights Food Hygiene Certificates, Street Trading Licence, DBS, Event Safety Management Plan, Water Quality Testing Laboratory Reports, PL / EL Documents))	CY + 6 ?	Paper and electronic	Corporate	Retain previous 3 years in office location and archive
10.5.2	Allotment Strategy	10 year strategy	Electronic & Paper Record	Corporate	Electronic copy retained on file
10.5.3	Allotment Tenancy Agreement	During the lifetime of the tenancy plus 3 years	Paper	Corporate	Scanning project is planned during 2015/16
10.5.4	Park Strategy	During the lifetime of the strategy plus 3 years	Electronic		
10.5.5	External Grant Funding Agreement – eg, Lottery, NRF, Football Foundation	Retention period is as stipulated by the funding body plus	Original hard copies	Statutory	Legal requirement from funder Retain key component documents relating to major site investment/improvements as a technical supporting document

10.5.6	Parks Management Plan	Retain for life of Plan, eg 5 years	Electronic	Corporate	Retained in electronic
10.5.7	Lease Agreements – Concession	Retain for length of agreement plus 3 years	paper	Corporate	Note – many parks related lease documents will be held by Wigan Council Property Services
10.5.8	Parks Buildings User Agreements	Retain for length of agreement plus 3 years	Paper	Corporate	
10.5.9	Pitch Lettings – Annual Letting Agreement with the Football Club	Retain for current year plus 6	Paper	Corporate	
10.5.10	Weekly Fixture List	Retain for current year plus 6	Paper	Corporate	
10.5.11	Playing Pitch Strategy	Retain for life of Strategy, eg 5 years	Electronic	Corporate	Retained in electronic format
10.5.12	Bowling Rental Agreements	Retain for current year plus 6	Paper	Corporate	
<b>10.6</b>	<b>Greenspace Services – Grounds Maintenance</b>				
10.6.1	Legionella – Site Testing	10 years	Paper and electronic	Statutory – H&S guidelines	Retained in electronic format and stored centrally.
10.6.2	Risk Assessments – Site and Task	10 Years	Paper and electronic	Statutory – H&S guidelines	Retained in electronic format
10.6.3	Internal ISO Audit Records	5 Years	Paper and electronic	ISO	Depot inspections and internal audit currently paper based
10.6.4	External ISO Audit Records	5 Years	Paper and electronic	ISO	
<b>10.6.5</b>	Waste Transfer Notes	3 Years	Paper and electronic	Statutory	
10.6.6	Waste Carriers Certificates	3 Years	Paper and electronic	Statutory	
10.6.7	Fuel Usage Records	3 Years	Paper and electronic	Corporate	



10.6.8	Pesticide Usage Records	10 Years	Paper and electronic	Statutory – H&S guidelines	
10.6.9	Green Waste Produced	3 Years	Paper and electronic	Paper and electronic	
10.6.10	Staff Training Records	10 Years	Paper and electronic	Paper and electronic	
10.6.11	Customer Orders & Worktickets	3 Years	Paper and electronic	Paper and electronic	
10.6.12	Completed Worktickets	3 Years	Paper and electronic	Paper and electronic	
10.6.13	Customer Satisfaction Surveys	3 Years	Paper and electronic	Paper and electronic	
10.6.14	ISO 9001 Standards	3 Years	Paper and electronic	ISO	
10.6.15	ISO 14001 Standards	3 Years	Paper and electronic	ISO	
10.6.16	OHSAS 18001 Standards	3 Years	Paper and electronic	ISO	
10.6.17	Grounds Maintenance Specification	3 Years	Paper and electronic	Corporate	
10.6.18	COSHH Sheets	10 Years	Paper and electronic	Statutory – H&S guidelines	
10.6.19	Arb Highways Inspections	Current + 6yrs	Paper and electronic	Corporate	

## Section 11 Housing Services

Ref No	Title of Document [Local Name]	Retention Period	Current Format	Authority	Notes/Access
11.1	Grants and loans				
11.1.1	Grants and loans	Until allocated	Paper format	Corporate	Grants or loans which are awarded via

		archived space allows Until grant or loan conditions are met	Electronic format	Corporate	affordable housing schemes, property improvement schemes including empty properties, adaptations
--	--	--	-------------------	-----------	--

**PEOPLE DIRECTORATE**

**RECORDS MANAGEMENT POLICY  
AND SCHEDULE**

**Date written:** November 2013

**Date of next review:** November 2014

**Version 1**

## **Document Control**

<b>Organisation</b>	Wigan Council
<b>Title</b>	People Directorate Records Management Policy and Schedule
<b>Prepared by</b>	[REDACTED]
<b>Owner</b>	[REDACTED]
<b>Subject</b>	Providing reference and guidance for records management

<b>Document Approvals</b>		
<b>Version</b>	<b>Sponsor Approval</b>	<b>Date Approved</b>
1	[REDACTED]	14 <sup>th</sup> November 2013
	[REDACTED]	13 <sup>th</sup> November 2013

<b>Document Distribution</b>		
<b>Version</b>	<b>Date Distributed</b>	<b>Distribution Method</b>
1	18 <sup>th</sup> November 2013	Via email

# **Records Management Policy**

## **Introduction**

There is a need for the Directorate to improve records management to support our core functions, ensuring that accurate records are kept of the Directorate's decisions, actions and activities. High-quality records will help improve performance and ensure that decisions are based on sound information. Improving records management will support transparent and fair governance and oversight of all the Directorate's activities. Good records management structures will underpin improvements to the way in which information and knowledge are generated, shared and exploited for the benefit of the Directorate, Council and the community as a whole.

The underlying principle of records management is to ensure that a record is managed through its life cycle from creation or receipt, through maintenance and use to disposal.

Good records management relies on the following:

- the creation of appropriate records
- the capture of records (received or created) in record keeping systems
- the appropriate maintenance and upkeep of these records
- the regular review of information
- the controlled retention of information
- the controlled destruction of information.

Through adhering to these principles the Directorate will benefit from:

- records being easily and efficiently located, accessed and retrieved
- information being better protected and securely stored
- records being disposed of safely and at the right time

## **Scope**

This policy applies to all paper and electronic records created, received or maintained by staff in the course of carrying out the Directorate's functions and which are maintained for a set period to provide evidence of its transactions or activities.

## **Responsibilities**

All information should be accurately recorded, objective in nature and expressed in a professional manner. A person or their nominated representative have the legal right to see their records at any point whilst receiving a service and until the time that the record is destroyed, this is an individual's right of subject access under the Data Protection Act 1998

This policy covers any record whether it is created by the Council or received by it. It applies to all staff, whether they work on Council premises, those who are mobile

workers, or those who work at home. It includes elected members when they are working on Council business.

Every individual who conducts Council business must adhere to this policy, and to any subsequent procedure or other document produced either corporately or within the Directorate which is introduced to improve management of the Council's records.

The responsible officer for the policy is the Assistant Service Manager - Information Governance. Day-to-day responsibility for the records management policy development is the Records Manager.

The Directorate's Policy and Schedule will be available on Sharepoint, or similar resource available to all staff.

### **Paper and Electronic documents and records: creation, storage and management**

It is the Council's policy to increase wherever practical the use of electronic means to create, store and manage documents and ultimately records. Wherever it is practical and efficient to do so, information systems that are based on paper files will be migrated in a managed way to an electronic system.

Any electronic system intended to store or manage records will be assessed to ensure that information held within it can be migrated to a different source should the software / hardware become obsolete, where this is not possible, paper records should be stored securely within Council property or archived off site at Iron Mountain at an appropriate time where the records will no longer be accessed on a regular basis.

### **Information Audit**

The Directorate will undertake regular audits to identify all of the information held by the Directorate. All teams will participate in this audit, to ensure that records and documents continue to be identified and properly managed in accordance with the retention schedule.

The audit will also allow the Council to maintain a list of all information systems used in each department, so that an overview of different systems and storage can be maintained.

### **Retention and disposal**

Retention periods have been assigned after consideration of legal requirements, good practice guidance and the business needs of the Directorate. Further guidance has been taken from the LGCRS (Local Government Classification and Retention Scheme).

Any records which require adding, removing or amending from the Retention Schedule for the Directorate should be reported to the Records Manager.

Records must not be held beyond the retention period set down in the Directorate's schedule

Where a paper files needs to be stored off site until the retention period has elapsed, these should be sent to Iron Mountain. For advice and support for all paper archiving requirements please contact [REDACTED], Records Manager on 01942 [REDACTED]. Guidance is also available by clicking on the following link [Iron Mountain procedures](#).

Personal and financial information on paper must be shredded by council staff or disposed of using approved confidential waste processes. The Policy for Disposal of confidential waste is subject to change and the most recent policy is available by clicking this link [Disposal ConfidentialWastePolicy](#). Under no circumstances should documents be recycled or thrown away in normal rubbish bins.

Work is currently underway to purge historic electronic information within individual IT systems which should no longer be held, updates will be provided as this project progresses. For records entered in error advice should be sought from the IT team to ensure that information held electronically is deleted properly. When a client record is destroyed, a record must be kept showing details of what record has been destroyed and in relation to which retention schedule.

### **Processes and procedures**

Each team will have in place clear procedures for the management of records – these will include how information and records are created, classified, shared, transferred, stored and disposed of.

For record held within the directorate which are subject to wider Council policy for example information relating to Human Resources, Finance, Property and Health and Safety records please contact Tracy Richards for current policy advice.

Compliance with the records management policy and schedule will also support statutory and regulatory requirements specific to certain functions particularly where there is a requirement to keep records or participate with inspections or audits.

### **Relevant legislation and standards**

- Local Government Act 1972
- BS ISO 15489 Records Management
- BS 7799 Code of Practice for Information Security Management
- BIP 0008 Code of Practice for legal admissibility and evidential weight for information stored electronically
- Civil Contingencies Act 2004
- Freedom of Information Act 2000
- Data Protection Act 1998
- Environmental Information Regulations 2004
- Re-Use of Public Sector Information Regulations 2005

## People Directorate Schedule Index

### **Children's Services**

1. Adoption records
2. Child Protection records
3. Schedule 1 Offender records
4. Looked After/fostering records
5. Child in Need records
6. Youth Offending records
7. Young Carers Records
8. Pupil Records – Virtual Schools
9. Pupil Records
10. Child minding/Out of school clubs/Daycare
11. Special Educational Support records
12. Governors

### **Adult services**

13. Records for providing support or services to Adults
14. Records for providing support or services to people with a mental illness
15. Admissions and Exclusion records
16. Adult carer records
17. Carers expense claims
18. Appointeeship records

### **Residential Homes**

19. Adults and Children's Home management systems and documents
20. Documents relating to the running of the establishment

### **General**

21. Blue Badge records
22. Legal and Contracts
23. Financial Transactions Management
24. Asset Monitoring and Maintenance
25. Asset Acquisition and Disposal
26. Health and Safety – Inspections and Assessments
27. Emergency Planning
28. Statutory Returns
29. Policy, Procedures, Strategy and Structure
30. Information Management
31. Enquiries and Complaints
32. Quality and Performance Management
33. Publications
34. Council and Land Premises

### **Miscellaneous**

35. Minutes that fall outside of other categories
36. Information provided to the Independent Barring Board
37. Representations
38. Withdrawal of Representations
39. Monitoring records
40. Annual Reports
41. Precious documents
42. Social Work diaries



### Children's Services –Adoption

Ref No.	Description of Record	Retention Action	Example of Records
1.	Process involving individual case management of children and young people who have been adopted.	Destroy 100 years from DOB	<ul style="list-style-type: none"> <li>○ Child's Adoption record</li> <li>○ Step Parent Adoption records</li> </ul>
	Process involving individual case management of families or adults who have adopted children in their care	Destroy 75 years from closure if approved  Destroy 10 years from closure if not approved	<ul style="list-style-type: none"> <li>○ Approved Adopters records</li> </ul>
	Adoption enquiries	Destroy 5 years after closure if no further action required or add to child's adoption record using the same retention period.	<ul style="list-style-type: none"> <li>○ Access to file requests</li> <li>○ Post Adoption enquiries</li> <li>○ Adoption enquiries</li> <li>○ Non Agency adoption enquiries</li> <li>○ Other LA checks</li> </ul>

### Children's Services – Child Protection

Ref No.	Description of Record	Retention Action	Example of Records
2.	Process involving individual case assessment, investigation, management of children involved in child protection	Destroy 25 years from closure	<ul style="list-style-type: none"> <li>○ Child Protection records</li> <li>○ Family Support Records</li> </ul>
	Case Conference - not registered	35 years from closure	
	Case Conference - registered	75 years from 18th birthday or 15 years from date of death if child dies before 18th birthday	
	Section 47 enquiries and investigations	35 years from closure	
3.	Process involving summary case management of Schedule 1 Offenders.	To individual's 100 <sup>th</sup> birthday	<ul style="list-style-type: none"> <li>○ Records about Schedule 1 Offenders</li> </ul>

### Children's Services – Looked After

Ref No.	Description of Record	Retention Action	Example of Records
4.	Process involving individual case assessment, investigation, management of children and young people	75 years from 18th birthday or 15 years from the date of death if the child dies before 18th birthday	<ul style="list-style-type: none"> <li>○ Looked after child records</li> <li>○ Residential Care records</li> <li>○ Family Support records</li> <li>○ Privately fostered records</li> <li>○ Residence Order records</li> <li>○ Special Guardianship Records (if not in relation to an ex Looked After child – 10 years)</li> </ul>
	Process involving individual case management of families or adults who have fostered children in their care.	10 years from closure if approved  5 years from date of decision if not approved	<ul style="list-style-type: none"> <li>○ Recruited and family friend records</li> <li>○ Supported Lodgings records</li> </ul>
	Fostering enquiries	Destroy 5 years after closure if no further action required	<ul style="list-style-type: none"> <li>○ NFA fostering enquiries</li> <li>○ Other LA checks</li> </ul>

### Children's Services – Child In Need

Ref No.	Description of Record	Retention Action	Example of Records
5.	Children in need who have not been adopted or looked after or who have not been the subject of a child protection enquiry.	Destroy 10 years from closure	<ul style="list-style-type: none"> <li>○ Child In Need records</li> <li>○ Family Support records</li> <li>○ No further action records</li> </ul>

### Children's Services – Youth Offending

Ref No.	Description of Record	Retention Action	Example of Records
6.	Offender Records	On programme completion - 12 months  Pre court/Programme completion - 3 years/18 <sup>th</sup> birthday  Court Orders - 5 years/18 <sup>th</sup> birthday	
	Parent Case Records	On programme completion – 12 months	
	Victim case records	On programme completion after 12 months	

### Children's Services – Young Carers

Ref No.	Description of Record	Retention Action	Example of Records
7.	Young Carers records	10 years after closure	○ Young carer records

### Children's Services – Pupil Records

Ref No.	Description of Record	Retention Action	Example of Records
8.	Virtual Schools records	75 years from 18 <sup>th</sup> birthday or 15 years from date of death if child dies before 18 <sup>th</sup> birthday	○ Children in Care Education records

Ref No.	Description of Record	Retention Action	Example of Records
9.	Pupil records	Destroy 25 years from DOB	<ul style="list-style-type: none"> <li>○ Education Welfare records</li> <li>○ EWO Court records</li> <li>○ Work requests</li> <li>○ Prosecution records</li> <li>○ Education Supervision Order records</li> <li>○ Victim Records</li> <li>○ Child Protection pupil records</li> <li>○ Connexions and Careers records</li> <li>○ Inclusion records</li> <li>○ Early Support Key Working records</li> <li>○ Portage service records</li> <li>○ Child Protection pupil records</li> <li>○ Pupil Inclusion records</li> <li>○ PRS records</li> <li>○ Early Intervention and Prevention records</li> <li>○ Ethnic Minority Achievement records</li> <li>○ Restorative Solutions/YPDAT records</li> <li>○ Education Penalty notice records</li> </ul>

Ref No.	Description of Record	Retention Action	Example of Records
9.	Pupil records	Destroy 6 years from closure	<ul style="list-style-type: none"> <li>○ CAF Assessments</li> </ul>
		Retain current year plus 2 years	<ul style="list-style-type: none"> <li>○ Truancy Sweep records</li> <li>○ Attendance returns</li> <li>○ School level data analysis</li> <li>○ School Register check records</li> <li>○ Entertainment and Employment Licence records</li> <li>○ Matron Licence records</li> </ul>
		6 years after 18 <sup>th</sup> birthday	<ul style="list-style-type: none"> <li>○ Licence for child over 12 to train for a dangerous performance</li> <li>○ Licence for persons under 16 going abroad to perform for profit</li> </ul>

#### Child Minding/Out of school clubs/Daycare

Ref No.	Description of Record	Retention Action	Example of Records
10.	Child Minding/Child care/Out of School club records	Destroy current year plus 6 years	<ul style="list-style-type: none"> <li>○ Child Support Team records</li> <li>○ Right from the Start client records</li> </ul>
		Kept indefinitely for the life of the Setting.	<ul style="list-style-type: none"> <li>○ Child care live Setting information</li> </ul>

Ref No.	Description of Record	Retention Action	Example of Records
10.	Child Minding/Child care/Out of School club records	7 years from closure	<ul style="list-style-type: none"> <li>○ Child Minding and Out of School Club records</li> <li>○ Childminder visit reports, Network records, Action Plans, Training Plans, Ofsted reports</li> </ul>
		Recommend retention of the current report plus the previous one for 2 years	<ul style="list-style-type: none"> <li>○ Day care and child minding inspections</li> </ul>
		10 years from the date on which the records were made	<ul style="list-style-type: none"> <li>○ Day care and child minding complaints</li> </ul>

### Special Educational Support Records

Ref No.	Description of Record	Retention Action	Example of Records
11.	Process involved in assessing and providing individual support for children who have a need of special education support	Destroy 31 years from DOB	<ul style="list-style-type: none"> <li>○ SEN Pupil record</li> <li>○ Special Educational Needs Statements</li> <li>○ SSET Pupil record</li> <li>○ TESS Pupil record</li> <li>○ Educational Psychology Records</li> <li>○ Short breaks data</li> <li>○ Disability Hub records</li> </ul>

### Governors

Ref No.	Description of Record	Retention Action	Example of Records
12.	Minutes <ul style="list-style-type: none"> <li>○ Principal set – signed</li> <li>○ Inspection copies</li> </ul>	Permanent Date of meeting +3 years	
	Agendas	Date of meeting	
	Reports	Date of report +6 years	
	Annual Parents meeting papers	Date of report +6 years	
	Instruments of Government	Permanent	
	Trusts and Endowments	Permanent	
	Action Plans	Date of action plan +3 years	
	Policy Documents	Expiry of policy	
	Complaint files	Date of resolution of complaint +6 years	
	Annual Reports required by the Department for Education	Date of report +10 years	
	Proposals for schools to become, or be established as Specialist Status schools	Current year +3 years	



### Adult Services

Ref No.	Description of Record	Retention Action	Example of Records	Notes
13.	Process involved in assessing and providing individual support or services for all other people.	Destroy 10 years after closure.	<ul style="list-style-type: none"> <li>○ Learning Disability</li> <li>○ Physical Disability</li> <li>○ Sensory Disability</li> <li>○ Rehabilitation and Discharge</li> <li>○ Intermediate care</li> <li>○ Communication Support</li> <li>○ Drug and alcohol misuse</li> <li>○ Occupational Therapy</li> <li>○ Homecare</li> <li>○ Occupational Therapy</li> <li>○ Assistive Technology</li> <li>○ Supported Living and Accommodation</li> <li>○ Residential and Day Services</li> <li>○ Adult Placement/Shared lives</li> <li>○ Hospital Social Work Service</li> </ul>	Deprivation of Liberty records should be destroyed on closure unless Manager deems the case is complex in which case the record would be destroyed after 10 years

Ref No.	Description of Record	Retention Action	Example of Records	Notes
13.	Process involved in assessing and providing individual support or services for all other people.	Destroy 10 years after closure.	<ul style="list-style-type: none"> <li>○ Commissioning Team service</li> <li>○ Short term breaks records</li> <li>○ ICES records</li> <li>○ Brokerage case files</li> <li>○ Day Service Register</li> <li>○ Supported Employment records</li> <li>○ Supporting people records</li> </ul>	Deprivation of Liberty records should be destroyed on closure unless Manager deems the case is complex in which case the record would be destroyed after 10 years

### Adult Services

Ref No.	Description of Record	Retention Action	Example of Records
14.	Process involved in assessing and providing individual support for people with mental illness.	Destroy 20 years after closure.	<ul style="list-style-type: none"> <li>○ Mental health records</li> </ul>
15.	Case Files (including appeals) for admissions and exclusions	Destroy 10 years from last action	<ul style="list-style-type: none"> <li>○ Appeal files</li> <li>○ Exclusions files</li> </ul>
16.	Assessment under Carers (Recognition and Services) Act 1995	Recommend a minimum of 6 years after provision of service ceases	<ul style="list-style-type: none"> <li>○ Adult Carer records</li> </ul>
17.	Carer's expense claims	Destroy after 6 years plus current year	<ul style="list-style-type: none"> <li>○ Adult placement carer's expense claims</li> </ul>
18.	Appointeeship records	Destroy after 6 years plus current year	<ul style="list-style-type: none"> <li>○ Appointeeship records</li> </ul>

### Residential Homes – Adults and Children’s Services

Ref No.	Description of Record	Retention Action	Example of Records
19.	Summary management systems that manage children/adults housed by the local authority	Keep permanently	<ul style="list-style-type: none"> <li>○ Children’s/adults home Registers</li> <li>○ Admissions registers</li> <li>○ Discharge registers</li> <li>○ Supported Accommodation Records</li> </ul>
20.	Documents relating to the operation of the establishment	Destroy 25 years from closure of file	<ul style="list-style-type: none"> <li>○ Secure unit records</li> <li>○ Shift Plan records</li> <li>○ Staff rota’s/annual leave information</li> <li>○ Communication books</li> <li>○ Daily log books</li> </ul>

### Blue Badge Records

Ref No.	Description of Record	Retention Action	Example of Records
21.	Blue badge administration	Destroy 3 years after badge has expired	<ul style="list-style-type: none"> <li>○ Blue badge</li> </ul>

### Legal and Contracts

Ref No.	Description of Record	Retention Action	Example of Records	Notes
22.	Pre Contract Advice. The process of calling for expressions of interest.	Destroy after 3 years or 1 year after completion of contract.	<ul style="list-style-type: none"> <li>○ Expressions of interest</li> </ul>	
	The process involved in the development and specification of a contract.	<p><b><u>Ordinary Contracts</u></b> Destroy 6 years after the terms of contract have expired.</p> <p><b><u>Contracts Under Deal</u></b> Destroy 12 years after the terms of contracts have expired.</p>	<ul style="list-style-type: none"> <li>○ Tender specification</li> </ul>	For project files containing drafts leading to a final version these records can be destroyed.
	The process involved in the issuing and return of a tender.	Destroy after 3 years or 1 year after completion of contract.	<ul style="list-style-type: none"> <li>○ Opening notice</li> <li>○ Tender envelope</li> </ul>	
	Evaluation of Tender.	<ul style="list-style-type: none"> <li><input type="checkbox"/> <b><u>Ordinary Contracts</u></b> Destroy 6 years after the terms of contract have ended.</li> <li><input type="checkbox"/> <b><u>Contracts Under Seal</u></b> Destroy 12 years after the terms of contract have expired.</li> </ul>	<ul style="list-style-type: none"> <li>○ Evaluation criteria</li> </ul>	

Ref No.	Description of Record	Retention Action	Example of Records
22.	Successful tender document	<input type="checkbox"/> <u>Ordinary Contracts</u> Destroy 6 years after the terms of contract have expired.  <input type="checkbox"/> <u>Contracts Under Seal</u> Destroy 12 years after the terms of contract have expired.	<ul style="list-style-type: none"> <li>○ Tender documents</li> <li>○ Quotations</li> </ul>
	Unsuccessful tender documents	Destroy after 3 years or 1 year after completion of contract.	<ul style="list-style-type: none"> <li>○ Tender documents</li> <li>○ Quotations</li> </ul>
	Post Tender Negotiation The process in negotiation of a contract after a preferred tender is selected.	Destroy after 3 years or 1 year after completion of record.	<ul style="list-style-type: none"> <li>○ Clarification of contract</li> <li>○ Post tender negotiation minutes</li> </ul>
	The process awarding of contract	<input type="checkbox"/> <u>Ordinary Contracts</u> Destroy 6 years after the terms of contract have expired.  <input type="checkbox"/> <u>Contracts Under Seal</u> Destroy 12 years after the terms of contract have expired.	<ul style="list-style-type: none"> <li>○ Signed contract</li> </ul>
	Contract operation and monitoring	Destroy after 3 years or 1 year after completion of record.	<ul style="list-style-type: none"> <li>○ Service Level Agreements</li> <li>○ Compliance reports</li> <li>○ Performance reports</li> </ul>

Ref No.	Description of Record	Retention Action	Example of Records
22.	Management and amendment of contract	<p><u>(a) Ordinary Contracts</u> Destroy 6 years after the terms of contract have expired.</p> <p><u>(b) Contracts Under Seal</u> Destroy 12 years after the terms of contract have expired.</p>	<ul style="list-style-type: none"> <li>○ Minutes and papers of meetings</li> <li>○ Changes to requirements</li> <li>○ Variation forms</li> <li>○ Extension of contract</li> <li>○ Complaints</li> <li>○ Disputes on payment</li> </ul>
	The process of awarding tenancies in welfare housing	<p><u>(a) Ordinary Tenancy</u> Destroy 6 years after the terms of agreement have expired.</p> <p><u>(b) Tenancy Under Seal</u> Destroy 12 years after the terms of agreement have expired.</p>	<ul style="list-style-type: none"> <li>○ Signed Tenancy agreements</li> <li>○ Sealed tenancy agreements</li> </ul>

### Financial Transactions Management

Ref No.	Description of Record	Retention Action	Example of Records
23.	Management of the approvals process for purchase, including investigations	Destroy 7 years after the end of the financial year in which the records were created	<ul style="list-style-type: none"> <li>○ Appointments &amp; delegations</li> <li>○ Audit investigations</li> <li>○ Arrangements for the provision of goods and/or services</li> </ul>

Ref No.	Description of Record	Retention Action	Example of Records
23.	Identification of the receipt, expenditure and write offs of public monies	Destroy 6 years after the conclusion of the financial transaction that the record supports	<ul style="list-style-type: none"> <li>○ Allowances</li> <li>○ Work orders</li> <li>○ Invoices</li> <li>○ Credit card statements</li> <li>○ Cash books</li> <li>○ Receipts</li> <li>○ Cheque counterfoils</li> <li>○ Bank statements</li> <li>○ Subsidiary ledgers (annual)</li> <li>○ Journals (annual)</li> <li>○ Vouchers</li> <li>○ Billing spreadsheets</li> </ul>
	Process involving the provision and support for individuals using public transportation	Destroy 6 years after the conclusion of the financial transaction that the record supports	<ul style="list-style-type: none"> <li>○ Applications</li> <li>○ Card issue</li> <li>○ Rail warrants</li> </ul>
	Processes that balance & reconcile financial accounts	Destroy 2 years after administrative use is concluded	<ul style="list-style-type: none"> <li>○ Reconciliation</li> <li>○ Summaries of accounts</li> </ul>

#### Asset Monitoring and Maintenance

Ref No.	Description of Record	Retention Action	Example of Records
24.	Management systems that allow the monitoring & management of assets in summary form	Destroy 7 years after the conclusion of the financial transaction that the record supports	<ul style="list-style-type: none"> <li>○ Subsidiary asset registers</li> </ul>

Ref No.	Description of Record	Retention Action	Example of Records
24.	Process of reporting and reviewing assets status	Destroy 2 years after administrative use is concluded	<ul style="list-style-type: none"> <li>○ Routine returns and reports on asset status</li> <li>○ Inventories</li> <li>○ Stocktaking</li> <li>○ Surveys of usage</li> <li>○ Acquisition and disposal reports &amp; proposals</li> </ul>
	The process of maintaining assets	Destroy 7 years after last action	<ul style="list-style-type: none"> <li>○ Garden maintenance</li> <li>○ Cleaning</li> <li>○ Painting</li> </ul>
	The process of maintaining plant and equipment	Destroy 7 years after sale or disposal of asset	<ul style="list-style-type: none"> <li>○ Service records</li> <li>○ Plant files</li> </ul>

#### Asset Acquisition and Disposal

Ref No.	Description of Record	Retention Action	Example of Records
25.	Management of the acquisition (by financial lease or purchase) and disposal (by sale or write off) process for assets	Destroy after 6 years, if under £50,000 or 12 years if over £50,000, after all obligations/ entitlements are concluded	<ul style="list-style-type: none"> <li>○ Legal documents relating to the purchase/ sale</li> <li>○ Particulars of sale documents</li> <li>○ Board of survey</li> <li>○ Leases</li> <li>○ Applications for leases, licences &amp; rental revision</li> <li>○ Tender documents</li> <li>○ Conditions of contracts</li> <li>○ Certificates of approval</li> </ul>



### Health and Safety - Inspections and Assessments

Ref No.	Description of Record	Retention Action	Example of Records
26.	Process of inspecting equipment to ensure it is safe	Destroy 6 years from destruction of the equipment	○ Equipment inspection records
	Process of carrying out monitoring to ensure that the process is safe	Destroy 3 years from last action	○ Monitoring results
	Process to ensure safe systems of work	Retain until superseded or process ceases +1 year	
	Process to assess the level of risk	Destroy 3 years from last assessment	○ Risk assessment
	Processes that permit work	Destroy 1 year from last action	
	Process that records injuries to adults	Destroy 3 years from closure	○ Accident books
	Process that records injuries to children	Destroy 25 years from closure	○ Accident books

### Emergency Planning

Ref No.	Description of Record	Retention Action	Example of Records
27.	Process to develop the emergency/disaster plan for the local community	Documents continually updated	○ Business Continuity records ○ Emergency planning records
	Incident records	Keep until incident fully investigated and court case completed. In special circumstances keep permanently	○ Incident records

Ref No.	Description of Record	Retention Action	Example of Records
27.	Process of recording the results of the test for emergency/ disaster plan for the local community	Destroy 10 years after closure	

#### Statutory Returns

Ref No.	Description of Record	Retention Action	Example of Records
28.	The process of preparing information to be passed on to central government as part of statutory requirements	Destroy 7 years from closure	<ul style="list-style-type: none"> <li>○ Reports to central government</li> </ul>

#### Policy, Procedures, Strategy and Structure

Ref No.	Description of Record	Retention Action	Example of Records
29.	Activities that develop policies, procedures, strategies, and structures for the local authorities	Destroy 7 years from end date	<ul style="list-style-type: none"> <li>○ Policy, procedure, precedent, instructions</li> <li>○ Organisation charts</li> <li>○ Records relating to policy implementation and development</li> <li>○ Asset management plan</li> <li>○ Children's services plan</li> <li>○ Adults service plan</li> </ul>

Ref No.	Description of Record	Retention Action	Example of Records
29.	The process of monitoring and reviewing strategic plans, policies or procedure to assess their compliance with guidelines	Destroy 5 years from closure	
	The process of consulting the public and staff in the development of <b>significant</b> policies of the local authority	Destroy 5 years from closure	surveys
	The process of consulting the public and staff in the development of <b>minor</b> policies of the local authority	Destroy 1 year from closure	questionnaires

### Information Management

Ref No.	Description of Record	Retention Action	Example of Records
30.	The activity whereby standards, authorities, restraints and verifications are introduced and maintained to manage information effectively	Keep permanently	<ul style="list-style-type: none"> <li>○ Classification schemes</li> <li>○ Registers</li> <li>○ Indexes</li> <li>○ Authorised lists of file headings</li> </ul>
	The process that records the disposal of records	Destroy 12 years after last action	<ul style="list-style-type: none"> <li>○ Disposal certificates</li> <li>○ Records of destruction</li> <li>○ Off site storage records</li> </ul>
	Routine access to information requests	Destroy 3 years from closure Destroy 1 year from response	<ul style="list-style-type: none"> <li>○ FOI records</li> <li>○ SAR records</li> </ul>

Ref No.	Description of Record	Retention Action	Example of Records
30.	The process that determines retention periods for local authority records	Destroy 12 years after superseded	<ul style="list-style-type: none"> <li>○ Retention schedules</li> </ul>
	The process that controls the sharing of information between partners	Destroy 7 years from closure	<ul style="list-style-type: none"> <li>○ Data sharing protocols and agreements</li> <li>○ Fair processing notice</li> </ul>

### Enquiries and Complaints

Ref No.	Description of Record	Retention Action	Example of Records
31.	The management in summary form of enquiries and complaints directed to the Department	Keep permanently	<ul style="list-style-type: none"> <li>○ SMG Reports</li> </ul>
	The management of enquiries, submissions and complaints which result in significant changes to policy or procedures	Keep permanently	<ul style="list-style-type: none"> <li>○ Reports</li> <li>○ Correspondence</li> <li>○ Ombudsman Referral</li> <li>○ MP/Councillor Referrals</li> </ul>
	The management of detailed responses on departmental actions, policy or procedures	Destroy 5 years after administrative use is concluded	<ul style="list-style-type: none"> <li>○ Reports</li> <li>○ Correspondence</li> <li>○ Ombudsman</li> </ul>
	The management of routine responses on, policy or procedures	Destroy 2 years after administrative use is concluded	<ul style="list-style-type: none"> <li>○ Form letters</li> </ul>
	Procedures for dealing with complaints	Until superseded	
	Complaints	Two years from the date on which it was made	
	Representation/Complaints procedure	Recommend a minimum of 6 years after the last representation/complaint	

### Quality and Performance Management

Ref No.	Description of Record	Retention Action	Example of Records
32.	The process of monitoring or reviewing the quality, efficiency, or performance of a local authority service or unit	Destroy 5 years from closure	<ul style="list-style-type: none"> <li>○ Best value Review</li> </ul>
	The process of assessing the quality, efficiency, or performance of a local authority service or unit	Destroy 2 years from closure	<ul style="list-style-type: none"> <li>○ Assessment form</li> </ul>

### Publications

Ref No.	Description of Record	Retention Action	Example of Records
33.	Design	Review annually	
	Published work	Until superseded or out of date	<ul style="list-style-type: none"> <li>○ Leaflets</li> <li>○ Booklets</li> <li>○ Newsletters</li> <li>○ Questionnaires</li> <li>○ Handbooks</li> </ul>
	Templates (all types)	Keep up to date	

### Council and Land Premises

Ref No.	Description of Record	Retention Action	Example of Records
34.	Accommodation files	Keep up to date	
	Agreements Section 38/40	Life of agreement + 6 years	
	Car parking arrangements	Keep up to date	
	Deeds	Until property disposed of plus 12 years	
	Deeds of dedication	After 12 years weed to agreement and plan then review every 10 years. Destroy 12 years after disposal	
	Deeds Register	Keep up to date and review annually	
	Leases	6 years after cessation of lease	
	Maintenance	Life of ownership plus 15 years	
	Operations	According to subject: Accidents Contracts Health and safety Etc.	
	Section 52/106 Open space agreements	Review every 10 years	
	ID / entry system	Keep up to date	
	Staff car park permits	Keep up to date	
Staff forms (Some completed forms may be added to HR files and retained accordingly)	Keep up to date There are no paper HR files now and managers may need to keep some documentation e.g. sick notes. Further clarification of specific documentation should be sought from Tracy Richards.		

### Miscellaneous

Ref No.	Description of Record	Retention Action	Example of Records	Notes
35.	Minutes that fall outside of other categories	Destroy 3 years after meeting date or the municipal year in which meetings held	<ul style="list-style-type: none"> <li>○ Meetings to allocate responsibility, prepare actions plans etc.</li> </ul>	
36.	Information provided to the Independent Barring Board	Recommend a minimum of ten years (after removal from list if known)		
37.	Representations	Recommend 3 years after process concluded		
38.	Withdrawal of Representations	Recommend 3 years after date of withdrawal		
39.	Monitoring records	Recommend current year plus 2		
40.	Annual Reports	Destroy 3 years after report completed or under SOP as appropriate.	<ul style="list-style-type: none"> <li>○ Complaints Annual Report</li> <li>○ Better Care Higher Standards Charter</li> </ul>	Discretion to be used as to destruction
41.	Precious documents	Retain as per case file record or return to service user	<ul style="list-style-type: none"> <li>○ Passports</li> <li>○ Handwritten letters</li> </ul>	
42.	Social Work diaries	Destroy after 2 years	<ul style="list-style-type: none"> <li>○ Social Work diaries</li> </ul>	