Request

1. Please send me the current organizational structure of Council Wigan. I need a detailed presentation of all the organizational units of the office with an indication of the people in management positions responsible for a given area of activity.

2. Please also send me the current policy on processing personal data

Response

1. The Council's organisational structure is published in the Constitution available at Agenda for Constitution on Monday, 24th February, 2025, specifically item 7 SMT Structure January 2025.pdf; this provides details of the people responsible for the different areas of activity.

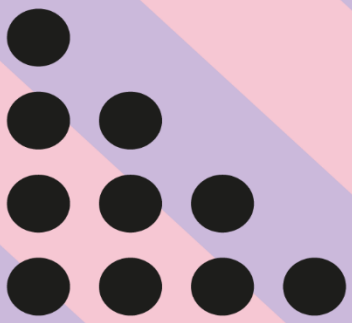
2. The Council has a Data Protection Policy that is attached; this sets out the Council's policy on processing personal data. The Council also publishes Privacy Notices on its website which explain to individuals how personal data is processed. The overarching Privacy notice is available at

   Wigan Council Primary Privacy Notice and service-specific Privacy Notices at –

   Privacy notices for all Council services.

Wigan Council

Data Protection Policy



Version 5.0 August 2024

Author: Graham Donelan
Date: 13th August 2024
Version 5.0

Document Title	Data Protection Policy
Purpose	To enable those working with information to have an effective understanding of their obligations regarding data protection compliance, confidentiality and data security.
Date of Approval	19th August 2024
Valid Until	19th August 2026
Owner	Data Protection Officer
Approver	Information Governance Operational Group (Chair – SIRO)
Distribution Method and Responsibility	Hub, Internal Comms, Cascade via IAOs Graham Donelan
Version	**Date** & **Comments**
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
5.1	May 2024, Biennial Review. First draft to IGOG.
5.0	August 2024, Approved by SIRO as Chair of IGOG

1. Purpose

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

2. Scope

This policy applies to ALL users of Council information and systems 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. Such demographic data items include, but are not limited to, name, address, NHS or NI Number, full postcode, date of birth, location data and online identifiers.

Special Category Data - This is personal data consisting of information such as race, ethnic origin, political opinions, health, religious beliefs, trade union membership, sex life or sexual orientation, biometric data and genetic data. Data relating to criminal convictions and offences is also offered additional protection in legislation. For more information about special category and criminal offence 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 UK GDPR and to the 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. This will help with a "data protection by design and by default" approach. 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 or pseudonymise 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

The Council will promote an understanding of the requirements of data protection legislation and 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 the Council processes 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 – this is known as data protection by design and by default. Departments 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 the Council 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 the Council uses personal data; it is renewed annually in 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 Data Breach Reporting process. 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 the most appropriate medium relevant to its core IT and Security strategy. This is predominantly in the cloud. Data is regularly backed up, aligned with the Council's IT strategy. 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 Council system 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 the request 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 IT 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 the Council holds 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 Assistant

Director Legal, Governance & Elections. There is a Deputy Data Protection Officer, currently the Service Lead – Strategic Lawyer Corporate.

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 IG Enabling Network which meets each month 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 other 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 Information Governance Team.

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 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.