Internal WMBC policies relating to retentions and backups that I expect to be disclosed under Freedom of Information	Please see attached PDFs.

Records Management Policy

Author: [redacted]
Date: 28th September 2022
Version 4.0

Version Control		
Document Title	Records Management Policy	
Purpose	To provide a framework for the efficient management of records to support the effective delivery of Council services, to promote transparency and accountability in decision making and to ensure legal obligations for retention and deletion of records are met	
Date of Approval	28th September 2022	
Valid Until	28th September 2024	
Owner	Deputy Chief Executive & Director of Resources & Contracts	
Approver	Information Governance Operational Group (Chair – SIRO)	
Distribution Method and Responsibility	Intranet and Internal Comms Update [redacted]	
Version	**Date**	**Comments**
1.1	27/06/08	Version for publication to all staff
2.0	10/10/11	Head of Legal and Risk
3.0	2016	GDPR working party
4.1	September 2022	Stakeholder consultation
4.2	September 2022	To IGOG
4.0	September 2022	Approved by IGOG

1. Purpose

To provide a framework for the efficient management of records to support the effective delivery of Council services, to promote transparency and accountability in decision making and to ensure legal obligations for retention and deletion of records are met.

2. Scope

2.1. Records are defined as recorded information created, received and maintained as evidence and as an asset by an organisation or a person, in pursuit of legal obligations or in the transaction of business. This definition is from the Code of Practice issued under section 46 of the Freedom of Information Act by the Secretary of State for Digital, Culture, Media and Sport providing guidance to public authorities on the keeping, management and destruction of records and is derived from BS ISO 15489.

2.2. This policy applies to 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. Throughout the remainder of this policy, these are called “staff”.

3. Core Principles

3.1. Where possible, records should kept in electronic format to enhance security, save space and reduce use of paper

3.2. Electronic records should be held on a case management system, other than in exceptional circumstances.

3.3. All electronic systems will have clear and robust processes for the saving and maintenance of records

3.4. Paper records must be kept in locked storage when not being used. If paper records have to be used at home, they must be kept secure at all times and particular care taken when transporting between the office and home.

3.5. All records must be included on the Record of Processing Activities/Information Asset Register

3.6. Records in any format must only be kept for the period specified in the corporate retention schedule

3.7. At the end of the retention period specified in the corporate retention schedule, action must be taken – retain for a further period, archive or destruction

4. Roles and Responsibilities

4.1. Overall responsibility for the management of corporate records sits with the Deputy Chief Executive & Director of Resources and Contracts

4.2. Assistant Directors, as Information Asset Owners, are responsible for

- 4.2.1. Ensuring local procedures are in place to comply with this policy
- 4.2.2. Ensuring appropriate level managers are allocated day-to-day oversight of specific records and case management systems
- 4.2.3. Ensuring that all staff in their area understand their responsibilities under this policy and are provided with training, as necessary
- 4.2.4. The completion and maintenance of the Record of Processing Activities and Information Asset Register for their area
- 4.2.5. Ensuring that records are reviewed against the corporate retention schedule

4.3. All staff are responsible for

- 4.3.1. Managing information they create and receive on a daily basis in line with this policy
- 4.3.2. Ensuring records are saved to a case management system, other secure location on the Council network or in paper form, if necessary
- 4.3.3. Taking care when creating records to ensure accuracy of information
- 4.3.4. Undertaking any training made available to support their management of records.

5. Security

5.1. Records (and the information therein) will be protected from loss of confidentiality, integrity and availability through the implementation of appropriate measures, including technical and organisational measures

5.2. Staff must comply with any such technical and organisational measures, including the ICT Acceptable Use Policy and the Information Security Policy

5.3. New case management and other record-keeping systems and processes must be reviewed for Information Security and Information Governance compliance via the ICT and Information Governance teams respectively. If a case management system is not available, this should be recorded with and agreed by the Information Governance Team

6. Retention and Deletion

6.1. Each directorate will maintain a retention schedule which will form part of the corporate retention schedule

6.2. All records should be maintained and reviewed in line with the corporate retention schedule

6.3. Ephemeral and trivial information (i.e. that which does not form part of a record) can and should be deleted or disposed of securely as soon as possible

6.4. Records to be deleted in line with the corporate retention schedule must be disposed of securely and permanently

6.5. Where a record has been destroyed, this should be able to be explained either by reference to the corporate retention schedule or a record of its destruction.

7. Business Continuity

Given the centrality of the Council's records to service delivery and decision making, the Council's Business Continuity Management Plan includes provision for the early restoration of core records following a disruptive incident or emergency. This will focus on records essential to deliver critical functions and contracts.

8. Key legislation and Council policies

8.1. There is no single piece of legislation governing records management. Specific legislation guides some of the retention periods in the corporate retention schedule and the following are relevant to the overall management of records or provision of information

8.1.1. Local Government Act 1972, Part VA
8.1.2. Local Government Act 2000, s22
8.1.3. Freedom of Information Act 2000
8.1.4. Environmental Information Regulations 2004
8.1.5. Civil Contingencies Act 2004
8.1.6. Data Protection Act 2018
8.1.7. UK General Data Protection Regulation 2021

8.2. The following Council policies should be considered in conjunction with this policy

8.2.1. Information Governance Framework
8.2.2. Information Security Policy
8.2.3. Data Protection Policy
8.2.4. Information Rights Policy
8.2.5. ICT Acceptable Use Policy
8.2.6. Business Continuity Management Plan
8.2.7. E-mail Management Policy

9. Review of this policy

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

Backup Policy

Document Classification:	Agilisys Internal
Document Ref.	IMS-DOC-A12-5
Version:	1.3
Dated:	02 March 2021
Document Author:	[redacted]
Document Owner:	

Revision History

Version	Date	Revision Author	Summary of Changes
1.0	03/08/2017	[redacted]	Initial Draft
1.1	30/11/2018	[redacted]	Review and minor updates
1.2	13/01/2020	[redacted]	Review and minor updates
1.3	02/03/2021	[redacted]	Annual review – minor changes

Distribution

Name	Title
[redacted]	Service Director
[redacted]	Projects and Programme Director
[redacted]	Partnership Director

Approval

Name	Position	Signature	Date
[redacted]	Partnership Director		03/08/2017
[redacted]	Service Director		03/08/2017
[redacted]	Service Director		30/11/2018
[redacted]	Service Director		13/01/2020
[redacted]	Service Director		02/03/2021

Contents

1 Introduction

The purpose of this document is to set out the way in which backups of information, software and system images are carried out, including regular testing.

Agilisys invests a significant amount of resources in collecting, processing and managing information about all aspects of its business operations, including customers, suppliers, employees, legal and financial. In order to ensure the integrity and availability of this information it is essential that a sound backup policy is adopted which takes due account of the classification of the information involved.

Without complete and usable backups, the organisation is exposed to an unacceptable level of risk and may be subject to significant legal consequences.

This document should be read in conjunction with the organisation's business continuity plans which deal with how backups are used to restore data in the event of a disaster, and the following additional documents:

- *Information Management Policy*
- *Information Security Policy*
- *Capacity Plan*

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Agilisys systems.

2 Backup Policy

Regular backups of essential business information must be taken to ensure that the organisation can recover from a disaster, media failure or other form of error.

An appropriate backup cycle must be designed and used that meets business requirements, complies with Agilisys information security policy and is fully documented. Third parties that store organisation information must also be required to ensure that the information is backed up appropriately.

In a cloud environment where the cloud service provider (CSP) is responsible for backups, the following criteria should be defined and agreed:

- Scope, schedule and location of backups
- Backup methods and data formats
- Retention periods for backups
- How the integrity of backups will be verified
- Restoration and testing procedures, including restoration timescales during a disruptive event
- Use of encryption
- How backups are segregated in a multi-tenant cloud environment
- Frequency and method of reviews of backup and recovery procedures

For backups under Agilisys control, full documentation, including a complete record of what has been backed up must be stored at an off-site location in addition to a copy at the site of origin.

The off-site location must be sufficiently distant from the site of origin of the backup to avoid being affected by any disaster that takes place at the main site.

Full documentation of the recovery procedure associated with each backup must be created and stored.

Monthly restore reviews of information restored from back up media must be performed to verify the reliability, accuracy and integrity of the back-up media and the restore process.

Removable media (e.g. tapes, external drives) must be protected in accordance with the Agilisys *Information Security Policy* to prevent damage, theft or unauthorised access.

Storage media being stored or transported must be protected from unauthorised access, misuse or corruption in accordance with the relevant *Information Security and Information Management Procedure*. Where couriers are required a list of reliable and trusted couriers should be established. If appropriate, physical controls such as encryption or special locked containers should also be used.

System documentation also must be protected from unauthorised access (this does not include generic manuals that have been supplied with software). Effective version control should be applied to all documentation and its storage.

Storage media that is no longer required must be disposed of safely and securely as specified in the document *Information Management Policy* to avoid data leakage, particularly where personally identifiable information (PII) is involved.

Appropriate arrangements must be put in place to ensure future availability of data that is required beyond the lifetime of the backup media.