Appendix 2

Records Management Policy

Version 3.0 – November 2023

1.0 Purpose of this policy

1.1 This document sets out the council-wide policy for records management standards that should be adhered to by all staff working with Wyre Council (the council) records.

1.2 All employees of the council have a responsibility to effectively manage council records and manage them appropriately in a way that meets the council's legal obligations.

2.0 Introduction

2.1 Any evidence of council business activity is a record. Records, therefore can be paper documents, electronic files, emails, databases, maps or images.

2.2 Records are the council's corporate memory and provide the evidence of its business actions and decisions. They also provide evidence that the council has satisfied statutory requirements. Well-managed records can improve the process of decision-making and facilitate business administration. They are, therefore, a corporate asset.

2.3 A record is a piece of information that has an intrinsic worth, which makes it important enough to save and keep secure for its evidential value. In order to decide whether a piece of information is a record or not, its business context must be understood as well as its relevance and significance to the organisation. If a record is of value as evidence of business activity, it is important that it be managed in a way that ensures the record:

- can be easily and quickly retrieved;
- is authentic - it is what it purports to be;
- is reliable - information in the record is accurate and can be depended on;
- has integrity – it is complete and unaltered;
- has appropriate context information about where it was used and why; and
- has structure so that the record is intact.

3.0 Relevant legislation

3.1 The council is committed to continuously improving the way it responds to requests for information under statutory access regimes. This includes the Freedom of Information (FOI) Act 2000, the Data Protection Act (DPA) 2018, the UK General Data Protection Regulation (UK GDPR) and the Environmental Information Regulations (EIR) 2004. Compliance however, is reliant upon proper management of the council's information, which needs to be managed, stored securely and easily located.

3.2 The DPA and the UK GDPR requires all organisations that handle personal information to comply with six principles regarding privacy and disclosure. Particularly relevant to records management is the fifth principle, which states that “Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed”.

3.3 The Local Government (Records) Act 1962 gave local authorities limited discretionary powers to hold their records in local archives. In particular, it states that “A local authority may do all such things as appear to it necessary or expedient for enabling adequate use to be made of records under its control”.

3.4 The Local Government Act (LGA) 1972 sets out the basic requirement for local authorities to ‘make proper arrangements’ to keep good records.

3.5 Reference to the following legislation and guidance may also be required when reading this policy.

- Computer Misuse Act 1990
- Human Rights Act 1998
- Public Records Act 1958 and 1967
- Local Government (Access to information) Act 1985
- Records Management Standards and guidelines British Standards (BSI)
- Lord Chancellors’ Code of Practice on Management of Records issued under S.46 of the Freedom of Information Act 2000

3.6 This list is not exhaustive and there will be other record-keeping legislation specific to certain areas of work, which should also be taken into account.

3.7 Reference to the following internal council documents may also be required when reading this Policy;

- The Council’s Constitution
- Employee’s Code of Conduct
- ICT Service Desk Computer Use Policy and User Agreement
- Security Incident Policy
- Data Protection Policy
- Data Classification Scheme
- Password Policy and User Guidance

4.0 Objectives

4.1 The aim of this policy is to define a framework for managing the council’s records to ensure that the council:

- creates and captures accurate, authentic and reliable records;

- maintains records to meet the authority's business needs;
- disposes of records that are no longer required in an appropriate manner;
- protects vital records;
- conforms to any legal and statutory requirements relating to record keeping, retention and disposal; and
- complies with government directives.

4.2 Whether acting as a data controller in its own right, or in common, or on another's behalf as a data processor, the council will maintain a record of its processing activities and make this available to the Information Commissioner's Office (ICO) on request. Information concerning the processing of personal data in respect of which the council is a data controller, will be communicated by the council to data subjects by means of the council's overarching privacy notice and also service specific privacy notices. These are located on the council's website.

https://www.wyre.gov.uk/service-area-privacy-notices/privacy-notice?documentId=108&categoryId=20133

4.3 The council is committed to ensuring compliance with data processing legislation and will:

- respect the rights of each individual;
- be open and honest about the data it holds;
- provide training and support to officers responsible for the handling of personal data in the course of their duties;
- notify the ICO annually, that it processes data. This is a statutory requirement and notification must be kept up to date with any changes to the use of personal data being updated within 28 days (the council has two registration numbers Z5682712 (General processing) and ZA319367 (Electoral Registration) and;
- inform the ICO and in some instances the data subject of any data breaches.

5.0 Data Classification Scheme (DCS)

5.1 An important element of records management is classification. ISO 15489 defines classification as the "systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system".

5.2 The council's DCS features three classification categories; unclassified, protected and restricted. The DCS sets out the criteria and controls required when handling and processing council data.

6.0 Information Asset Registers (IAR)

6.1 Each service area within the council should have in place an up-to-date 'live' IAR. The register should set out the details of the information asset, its classification (as per the DCS), the council's legal basis for processing (if personal/sensitive data), the format it is held in (electronic or paper), the named Information Asset Owner (IAO), it's location and its retention period. There is a standard template for IAR's held on the HUB.

6.2 IAR's are subject to regular review by Internal Audit and spot checks may be carried out by the Data Protection Officer (DPO). However, it is the responsibility of the Head of Service (HOS) and/or Service Manager and any nominated IAO's to ensure that the register is reviewed regularly and kept up-to-date.

6.3 During the Pandemic it became necessary in some services to use various social media platforms e.g. WhatsApp to process council data. Whilst the need to use alternative platforms has now diminished following a return to 'business as usual', a review of the continued use of alternate systems will be carried out in early 2024. An instruction has been cascaded to managers informing them that if individual services are continuing to use alternative systems such as WhatsApp to process council data, they should document this in their information asset registers to allow information requests to be answered correctly.

7.0 Roles and responsibilities

7.1 Senior Information Risk Owner (SIRO)
The Chief Executive serves corporately as the council's named SIRO in relation to information governance and data security related matters. The SIRO forms part of the council's Corporate Management Team (CMT) and therefore has a firm understanding of the strategic business goals of the council. They also understand how these goals may be impacted by information risks and how those risks may be managed. The SIRO's duties include; taking ownership of the organisation's risks registers, acting as a champion for information risk at CMT and directing the work of the council's DPO.

7.2 Data Protection Officer (DPO)
The DPO's minimum tasks, as defined by legislation are:

- to inform and advise the council and its employees about their obligations to comply with the UK GDPR and other data protection laws;
- to monitor compliance with the UK GDPR and other data protection laws, including managing internal data protection activities;
- advise on data protection impact assessments;

- train staff and conduct internal audits; and
- to be the first point of contact for supervisory authorities (ICO, Local Government Ombudsman) and for individuals whose data is processed (residents, employees, customers etc.).

7.3 Heads of Service (HOS) / Managers

HOS/Managers are ultimately responsible for the management of the records within their services, in accordance with this policy and for ensuing that their staff are aware of any data sharing protocols and storage and retention periods documented in the council's IAR's. HOS/Managers will be asked to make an annual declaration to the DPO to confirm that their services IAR have been reviewed and updated and that checks have been made to ensure the necessary technical measures are in place to protect the council's assets.

7.4 Information Asset Owners (IAO)

All council employees are responsible for creating and maintaining records in relation to their work that are authentic, up-to-date and reliable. However, service areas may also have individual nominated IAO for a specific system or a collection of records. IAO's ultimately have the necessary knowledge and skills to ensure that the asset is managed correctly and if not, to take the necessary action if any deficiencies in the relevant processes are identified. The IAO's core responsibilities are as follows:

- to ensure the capture of records is accurate and provides evidence of the service's activities;
- to make every effort to provide reliable data and records management;
- to observe and support any corporate polices and procedures;
- to understand any risks associated with processing and be pro-active about mitigation;
- to ensure that any contractors or third parties with access to council records are managing them in accordance with council policy and contracts/service level agreements, and;
- to provide the DPO with an annual declaration to confirm compliance with the terms of any written contracts or data sharing agreements and that the necessary technical measures are in place to protect the data being processed.

7.5 Information Governance Group (IGG)

The council has an IGG that meets formally approximately every 2 months. The membership is made up of the council's DPO and Deputy, ICT Service Manager, Legal Services Manager and Legal Executive. Other council officers are invited on an ad hoc basis depending on the agenda items. The group has an agreed terms of reference, which is reviewed annually. The group is responsible for the annual review of the council's information governance policies and procedures, prior to formal approval by the Audit and Standards Committee. All meetings have an agenda and are minuted by means of an action plan which documented any agreed actions. The action plan(s) is/are submitted to the SIRO through CMT on a quarterly basis.

7.6 ICT Service Manager (ICTSM)
The ICTSM is responsible for ensuring that all council ICT systems are designed and maintained to meet the council's security, records management and data protection obligations, and to ensure that they are strategically and operationally fit for purpose. The ICTSM is responsible for updating the IGG regarding any issues concerning the security of the council's systems and the records within them.

8.0 General record creation and record keeping

8.1 Each service area must have in place adequate record keeping systems (paper or electronic) that document its activities and allow for quick and easy retrieval of information. It must also take into account any legal / regulatory requirements specific to the area of work. Systems should include:

- records arranged and indexed so they can be easily retrieved by any officer at any time;
- clear and documented procedures are in place for keeping the system updated;
- procedures and guidelines for referencing, indexing and version control;
- the ability to cross reference electronic and paper records; and
- documented procedural notes on how to use the system.

8.2 Details of these records should be documented in the individual services IAR which should be treated as a 'live' document, ensuring that when the data being held changes or moves, the IAR is updated to reflect this.

9.0 General record maintenance and security

9.1 Any record keeping system must be maintained so that the records are properly stored and protected and can easily be located and retrieved. This will include:

- ensuring that adequate storage accommodation is provided for records and they are kept clean and dry;
- monitoring the movement and location of records so that they can be easily retrieved and provide an audit trail;
- controlling access to the information, ensuring that all staff with access are aware of the arrangements for allowing access to certain types of information;
- identifying vital records and applying the appropriate protection and back-ups, which should be documented in individual business continuity plans; and

- ensuring non-current records, which are to be retained in accordance with individual IAR’s are transferred in a controlled manner to a safe, secure archive facility, rather than being stored in offices.

10.0 Record retention and disposal

10.1 With increasing public access to our records, it is important that disposal of records happens as part of the managed process and is adequately documented.

10.2 HOS/Managers must have in place clearly defined arrangements for the selection of records for disposal, and for recording this work. The system should ensure that:

- records are reviewed and disposed of/transferred to an appropriate archive facility in accordance with the services individual IAR and any other published regulatory or statutory retention requirement;
- records subject to FOI/EIR and Subject Access Requests (SAR) are not destroyed. It should be noted that it is an offence to alter or destroy records with the intention of preventing disclosure;
- an intended disposal/review date must be captured when creating electronic records. Furthermore, care must be taken when procuring an electronic system to ensure the system has the necessary capabilities to allow for on-going retention processes; and
- documentation of the disposal/transfer of records is completed and retained.

11.0 Emails

11.1 Emails are stored in Microsoft's UK facility that incorporates multiple levels of redundancy. This allows users to delete emails to their recycle bin, which are then recoverable for 14 days. There is a second stage recovery area, which allows recovery of emails for a further 30 days by a system administrator.

11.2 Any emails permanently deleted by users are recoverable up to the point at which the council implemented their current backup solution (May 2021). The system is configured to back up a maximum of 7 years of data and will then continue to back up on a rolling basis, aging and deleting data beyond this retention period.

11.3 An email warning is issued to users if they are reaching capacity in their mailbox. Users are encouraged to regularly housekeep their mailboxes so that they do not reach capacity limit. Managing emails with attachments, creating a filing system and refraining from leaving items in their inbox, sent items or deleted folders are suggested methods for good housekeeping techniques.

12.0 Corporate CXM system

12.1 There are many different systems across the organisation supporting the council's activities. These are all, by definition, records management systems. In addition, the council is continuing to move forward with a corporate CXM system that either complements other council systems, serves to migrate unstructured data alongside these systems, or in some cases actually replaces these systems. The CXM administrator provides an annual declaration to the DPO to confirm they are satisfied that there are sufficient technical measures in place to protect the information held within the system.

13.0 Storing records offsite / hybrid working

13.1 All records that are taken and held offsite should be managed in accordance with this Policy, the council's Data Protection Policy, the DCS and individual service IAR.

Formatted: Indent: Left: 0 cm, First line: 0 cm

14.0 Contract clauses

14.1 The council's Legal Services Team in conjunction with the appropriate HOS/Manager and DPO will strive to ensure that any contracts with third party data processors have appropriate data protection, UK GDPR and record management clauses regarding the agreed and approved methods of information handling and storage and, if relevant, set out how information will be transferred back to the council at the end of a contract.

15.0 Training and awareness

15.1 Since all council employees will at some point be involved in creating, maintaining and using records, it is vital that everyone understands their responsibilities in relation to data security and their record management responsibilities that are set out in this policy.

15.2 Managers need to ensure that staff responsible for processing and managing records are appropriately trained / experienced and that all staff understand the need for record management.

15.3 The council will run training courses to ensure that all staff are aware of their obligations regarding data protection, FOI, EIR, SAR and general records management. These courses are considered mandatory and HOS/Managers should allow and support their staff in attending and completing the necessary training and awareness sessions being provided.

16.0 Reviewing the policy

16.1 This policy will be maintained and reviewed annually by the IGG and CMT (which includes the SIRO) before being formally approved by the council's Audit and Standards Committee.