HUMBERSIDE FIRE AND RESCUE SERVICE

Service Improvement

Records Management and Data Quality Policy

Owner	**Executive Director of Corporate Services**
Responsible Person	**Head of Corporate Assurance**
Date written	**April 2018**
Last review	**July 2023**
Date of next review	**August 2024**
EIA Completed	**May 2021**

What we must do well

How we support our communities

We value and support the people we employ

We efficiently manage the Service

CONTENTS

1. INTRODUCTION

Records management is vital to supporting the Humberside Fire & Rescue Service's (HFRS) daily operations. Effective records management helps ensure that we have the right information at the right time to make the right decisions. Data quality is crucial to this, and the availability of complete, accurate and timely data is vital to deliver services, evidence service improvements and provide good/effective governance.

The Service is committed to creating, keeping and managing records which document its principal activities. Increasing reliance is placed on information and the need for reliable data has become more critical. Good quality data is essential for supporting decision making and the Service needs arrangements in place to ensure the quality of its data. These records are the Service's corporate memory.

To maximise our potential, records must be accurate and of a high quality, in order for staff to be able to trust the records they use. Records will be retained for as long as they are required for legislative, business, accountability, or cultural purposes. They will be stored in a manner and location that enables the Service to have an appropriate level of control over their management and be disposed of appropriately. Where Service records are shared with other organisations, it will be done in a lawful and secure manner.

The Service will follow agreed practice and comply with all legislative requirements with regard to the creation, storage and management of its records.

Compliance with this policy will help the Service meet its statutory obligations under the Local Government Act 1972, the Lord Chancellors Code of Practice on the Management of Records (issued under s46 of the Freedom of Information Act 2000) and ensuring legal compliance with the Freedom of Information Act 2000 and data protection legislation.

Core Code of Ethics

HFRS has adopted the Core Code of Ethics for Fire and Rescue Services. The Service is committed to the ethical principles of the Code and strives to apply them in all we do, therefore, those principles are reflected in this Policy.

National Guidance

Any National Guidance which has been adopted by HFRS, will be reflected in this Policy.

2. EQUALITY AND INCLUSION

HFRS has a legal responsibility under the Equality Act 2010, and a commitment, to ensure it does not discriminate either directly or indirectly in any of its functions and services nor in its treatment of staff, in relation to race, sex, disability, sexual orientation, age, pregnancy and maternity, religion and belief, gender reassignment

or marriage and civil partnership. It also has a duty to make reasonable adjustments for disabled applicants, employees and service users.

3. AIM AND OBJECTIVES

The aim of this policy is to make sure the Service's record management is effective and compliant with legislation, by ensuring:

- All records in the Service's possession are properly created, stored, used and considered by all staff as an essential asset to the organisation.
- Information is held in line with data protection legislation and the Service's Data Protection Policy.
- Data quality is improved, and processes are in place which evidence the importance placed upon data quality by the Service.
- The Service and its employees understand records management practices.
- The Service operates an Information Asset Register (IAR).
- Records are retained for no longer than necessary and archived or destroyed in accordance with Retention Schedules.

4. ASSOCIATED DOCUMENTS

- **Equality Impact Analysis** (EIA/OD)
- **Legal References**
  - Code of Practice on (1) The Management of Records of Relevant Authorities
  - Freedom of Information Act 2000, Section 46 Code of Practice – records management
  - Code of Practice on the discharge of the obligations of public authorities under the Environmental Information Regulations 2004
  - Freedom of Information Act 2000
  - Data Protection Act 2018
  - UK General Data Protection Regulation (UK GDPR)
  - Re-use of Public Sector Information Regulations 2005 Information
  - Information Commissioners Office
- **National Guidance**
  There is no specific National Guidance relevant to this policy.
- Information Classification Policy
- Information Security Policy
- Disposal and Destruction of Records Policy Delivery Guidance

5. DEFINITIONS

There are other policies which provide guidance regarding ICT security and data protection. For the purposes of this policy, the following definitions are in relation to records management.

Records Management: the supervision and administration of digital or paper records, regardless of format. Records management activities include the creation or receipt (including data quality) storage, use and disposal of records.

Record: information created, received and maintained as evidence and information by an organisation or person in pursuance of legal obligations or in the transaction of business. This includes records in all physical and electronic formats, including, but not restricted to:

- CDs, DVDs, Blu-Ray
- Databases and spreadsheets
- Electronic documents
- Emails
- MS Teams Chat
- Paper files/documents
- Microform, including microfiches & microfilm
- Published web content (Intranet/Internet/Extranet), including records created in social media used for business purposes
- Records stored on removable media, such memory sticks
- Visual images, such as photographs
- Audio, such as voicemail

Information Asset Owner (IAO): a mandated role, the individual appointed is responsible for ensuring that specific information assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited. In HFRS, this responsibility will normally be assigned to Heads of Function.

Information Asset Register (IAR): a list of all the personal and non-personal information assets (records) held by the Service.

Senior Information Risk Owner (SIRO): the individual with overall responsibility for the Service's information risk. IAOs report to the SIRO.

Retention Period: the identified period of time for which each information asset will be held.

Retention Schedule: a document detailing the retention period for each information asset, the justification for that retention period and what will happen to the record at the end of the retention period.

6. CORPORATE REQUIREMENTS

Records and information are vital to the effective operation of the Service. Records are the basis on which decisions are made, services provided, and policies developed. Effective records management supports the Service's work in all areas.

The Corporate Assurance Section are responsible for ensuring the records management function is adequately supported and are available to provide advice and a discussion forum for matters relating to information governance.

The Strategic Leadership Team are responsible for overseeing the drafting, compliance and communication of policies and guidance relating to information management.

To ensure compliance, Heads of Function are designated as IAOs and are responsible for ensuring the effective management of records and data quality within their service areas and adherence to this policy. IAOs may nominate members of staff of sufficient seniority to take lead responsibility for records management in their respective service area. IAOs ensure that access to their information assets is appropriate and up to date, taking in to account the Data Protection Policy and the need to protect personal data.

The SIRO will oversee the work of all IAOs ensuring compliance with this policy. Corporate Assurance will ensure that the IAR is available to the SIRO, and if required, the Data Protection Officer (DPO) to demonstrate compliance with data protection legislation, specifically the required records of processing activity and the Service's Data Protection Policy.

All staff are required to support IAOs in respect of their records management duties. They should actively monitor compliance with this Policy, ensuring that records are created and filed in line with the agreed filing convention and appropriate classification. Retention and disposal schedules, including schedules of documents for transfer to Archives, are kept up to date and all disposal decisions are properly recorded, with a formal record of transfer maintained in accordance with the agreed procedure. IAO are responsible for ensuring information on the records within their area of responsibility are maintained in the Service's IAR.

Corporate automatic retention and deletion schedules have been set for the following applications:

- **Email** - An automatic retention schedule deletes emails on a monthly basis that are more than 3 year's old.
- **MS Teams** -
    - Individual chat automatic retention schedule deletes any chat over 30 days old.

- Teams Chat - automatic retention schedule deletes any chat older than 365 days (1 year).
- Files in Teams & channels - automatic retention schedule deletes documents older than 365 days (1 year) from the date last modified.

Managers should ensure that processes are in place to support employees in respect of creating and maintaining records. Consideration must be given to this policy, as well as to how records required for permanent preservation are transferred to Archives.

Employees are responsible for creating and maintaining records in relation to their work. All reasonable efforts must be made to ensure the quality of data, as all employees are responsible for the data they record. Employees must never knowingly record data which is inaccurate or incomplete. Records should be created and filed in line with agreed processes (including classifications, file naming conventions and appropriate designation in the header and footer).

All individuals need to be aware of their obligations relating to records as part of their Service duties. Failure to adhere to this policy can result in serious misconduct and could lead to disciplinary procedures or, the prosecution of employees.

7. MANAGING RECORDS

Records management is a core corporate function. The Service ensures that it creates the records it will need for its business. All records are recorded and presented in accordance with all relevant legal provisions, regulations and central standards.

The Service has timely access to all relevant information and records will only be kept for as long as is necessary to comply with legal, administrative and financial requirements.

All records will be properly titled, referenced and indexed; all records will be stored in accordance with the relevant storage system.

All records are authentic and reliable version control will be utilised to ensure that changes are recognised and considered during any decision-making process.

Data quality forms a fundamental part of any record. Robust processes must be in place to evidence how the Service meets common data quality standards (see Section 9).

All disposal decisions will be fully recorded and authorisation for disposal evidenced in line with agreed delegations.

Records required for permanent retention for evidential and historical purposes will be transferred to Archives, and the transfer decision and custody recorded.

Guidance and advice on record management is available from the Corporate Assurance Section.

8. DATA INVENTORY

IAOs will be required to ensure information regarding the records within their area is maintained in the Service's IAR. Information from that register will be made available to IAO to use as part of the risk-assessment process.

The IAR must be kept up to date and reflect changes including office moves, restructures, staffing changes and the procurement of new systems. The IAR must be reviewed at least annually by each IAO.

Individual pieces of information should be grouped into manageable portions. There is no need to assess every individual file and database entry; by grouping a set of information at an appropriate level you identify an information asset.

The IAR holds retention schedule information that sets out periods for which records should be retained. This is supported by the Retention Schedules which detail appropriate disposal actions and which records will be selected for permanent preservation.

The IAR is published on the portal and made available to all staff. The Retention Schedules are published on the portal, but also on the internet to ensure the Service is transparent in its use of information.

9. DATA QUALITY

Data quality is a fundamental part of the Service's approach to records management. Data will be regarded as high quality if it meets the following common data quality standards.

- Accurate (reflects what is being described/captured/copied)
- Valid (conforms to recognised standards, data reflects stable and consistent collection and the source is known).
- Timely (available when needed and within a reasonable time period).
- Relevant (only relevant data of value is collected, analysed and used).
- Complete (all relevant data is recorded).

Appendix A outlines in more detail the common data quality standards expected to ensure high quality data is recorded/used.

If anyone requires any further guidance or information relating to this document, please contact Corporate Assurance

APPENDIX A: COMMON DATA QUALITY STANDARDS CHECKLIST

1. Accuracy

- ✓ Data is sufficiently accurate for its intended purposes.
- ✓ Data should be captured once only, although it may have multiple uses.
- ✓ Data will be checked at the point of collection.
- ✓ Evidence that data has been checked and validated for accuracy should be available.

Example: When updating a service user's demographic data, the fields should be checked with the individual to ensure they are correct; this could include verbal communication with the individual or validation against existing data.

2. Validity

- ✓ Data should be recorded and used in compliance with relevant requirements, including the correct application of any rules or definitions.
- ✓ A consistent data collection process is used.
- ✓ Employees collecting data are suitably trained/supervised.
- ✓ Data should be from primary sources wherever possible.
- ✓ Any data quality issues are identified, assessed and rectified.

Example: A database extract contains the information which is needed for a report. The source of the extract is not clear or why it was created in the first place. In this scenario the information cannot be trusted, and the information should be extracted again or checked against the source database.

3. Timeliness

- ✓ Data should be captured as quickly as possible after the event or activity and must be available for the intended use within a reasonable time period.
- ✓ Data must be available quickly and frequently enough to support information needs and to influence decision making.

Example: Having visited a service user the relevant record is required to be updated. Should this not happen within a reasonable/pre-agreed timescale, the risk of unnecessary contact/intervention or inaccurate data being recorded increases.

4. Relevance

- ✓ Data captured should be relevant to the purposes for which it is used. If data is not required within a documented process, it should not be recorded.

Example: It is appropriate to record a service user's address within a record however it is not required, nor appropriate for their alarm code to be recorded.

5. Completeness

- ✓ Data requirements should be clearly specified based on the information needs of the organisation and data collection processes matched to these requirements.
- ✓ Monitoring missing, incomplete, or invalid records can providean indication of the level of data quality and can also identify any recording issues.

6. Summary

Considering all of the above factors, it should be possible to give a level of assurance about data quality in the organisation.