1253 Retention and version control policy

Effective information and records management is necessary to meet business objectives, comply with regulatory requirements, and to work efficiently. This policy explains the retention and version control procedures necessary to ensure that important Service information is accurate, available, up-to-date, and kept only as long as required.

Knowledge of this policy will enable staff to:

- Comply with legislative retention and disposal requirements
- Improve efficiency by only retaining relevant information
- Reduce the costs of storage and backup space
- Operate effective business processes and handle information requests
- Uphold the transparency and open government agenda

OWNER	**Information Compliance Manager**
LAST REVIEW	**March 2021**
REVIEW DUE DATE	**July 2022**
VERSION CONTROL/AMEND SCHEDULE	**16.0**

CROSS REFERENCES
Records Management Society guidance
National Archives Guidance

CONTENTS

PART 1 – POLICY SECTION

1. Policy Statement

Cheshire Fire and Rescue Service will retain authentic, reliable and usable records, which support business functions and provide evidence of activities for as long as required for operational reasons and to meet legislative requirements.

This requires key information to be formally and consistently managed using retention schedules, version control, and clear naming conventions.

This policy supports the suite of information management policies, by defining the principles to be applied through the information life cycle that will ensure that information is fit for purpose and handled appropriately, consistently and efficiently.

These procedures must be applied to all physical and electronic records, and consider back ups and mobile media.

2. Specific Commitments

The Service will follow a formal retention schedule for important or critical business information and records. This policy applies to any information or records that the Service relies on to:-

- support business processes,
- provide evidence of historical, current or projected activity or actions, or
- underpin Service accountability.

Information which is of short term facilitative value, unimportant or duplicated does not require formal handling and is out of scope of this policy.

Each department is responsible for operating local procedures that ensure their information is organised, easy to find, accurate, fit for purpose and complies with the increasing range of information legislation.

These procedures will include:-

- Retention
- Disposal
- Consistent naming and structured storage
- Version control

3. Ownership/Monitoring

Information Owners and Head of Department are responsible for implementing this policy and monitoring compliance with required standards.

The Information Officer will provide guidance and support to managers for information retention, disposal and version control.

All employees, including temporary and agency staff are responsible for handling Service information correctly.

PART 2 – PROCEDURE

1. Departmental procedures

Managers will implement local procedures and ensure the appropriate retention and disposal of any records required to satisfy legal, financial or other requirements of public administration.

These procedures will vary according to the situation but must ensure:-

- Specifying the essential information required – to ensure quality and completeness
- Detailed naming conventions – ensuring descriptive and consistent names of files to facilitate other version control and retention procedures
- Version control – to evidence authorisation and approved changes, and preserve/remove earlier versions
- Structured information storage - grouping information in order to facilitate searching, security or access levels, and retention periods
- Review of information – for validation and monitoring purposes
- Retention and controlled destruction of information.

NB prior to destruction information of historical significance should be offered to the Cheshire public Records Office by contacting the Information Officer.

2. Information retention requirements

The Service Retention Schedule (refer to guidance section) encompasses legislation and industry standards. Where there is no formal retention guidance the Service has defined the retention periods based on known business requirements.

These additional retention periods are based on whether the information:-

- Is needed to meet statutory or other regulatory requirements.
- Would be required as evidence in any potential dispute between 3rd parties, or on behalf of the Service, or against the Service.
- Has any operational implications for the Service, eg training, precedents, performance management or comparison purposes.
- Has historic or intrinsic value, eg major incidents

Any retention period implemented must not exceed Data Protection or other legal considerations, but other than this the Service can exercise discretion.

Where necessary the Department manager or information owner may operate a more detailed supplementary local department information list.

For information that is not included in the Service retention scheduled consult the Information Manager, who will seek guidance from the Records Management Society and The National Archives if necessary.

3. Disposal of information

Each department must keep sufficient evidence of records/information disposal. This will be relied on in the event of a query or formal information request, and may be a list, register or summary appropriate to the process operated.

Disposal by shredding is mandatory for confidential paper documents, strategic Service documents which are not published, and records containing personal information.

Recycling is important to the Service, but care must be taken to ensure that information security is considered prior to recycling paper documents.

IT are responsible for ensuring that IT equipment is properly cleansed of Service data prior to disposal.

If there is any investigation, information request or audit relating to the information, then the Departmental Manager will suspend any further disposal of documents until the situation is completed or resolved.

4. Storage space and archives

ICT provide storage space based on historical departmental usage. This is monitored to encourage review and removal of out of date, redundant and obsolete information. However necessary Corporate information must be retained by departments.

The Service does not operate a central archive because information is owned by departments and operates under a departmental structure. If departments require advice they should consult the Information Officer and IT.

The Cheshire Public Records Office should be offered information of historical interest that the Service no longer requires. Advice is available from the Information Officer.

PART 3 – GUIDANCE

1 Legislation and sector requirements

Fire and Rescue Services work in a regulatory environment involving a number of factors which influence information retention:-

- Business legislation and regulations, including but not limited to:
    - Data Protection Act 2018 (which imposes restrictions on retention and has additional information handling requirements)
    - Freedom of Information Act 2000
    - Environmental Information Regulations 2004
    - Criminal Justice Act 1988
    - Civil Evidence Act 1995
    - Local Government statutes – generally require permanent retention
    - The Limitations Act 1980 – generally retention for 6 years
    - Regulation of Investigatory Powers Act 2000
    - Human Rights Act 1998
    - Financial – VAT Act 1994, Taxes Management Act 1970

- Codes of practice such as:
    - Section 46 Freedom of Information Act Code of Practice for the management of records
    - National Audit Office - 6 years retention of accounts, supporting documents minimum of eighteen months from financial year end

Note supporting documents can be retained for 6 years in case of queries

- Public interest: documents of historic interest or intrinsic value should be considered for permanent retention and/or offered to the Cheshire Public Records Office. For guidance, consult the Information Manager.

- The Health and Safety at Work Act 1974.This requires special consideration because in the Fire and Rescue service because it is implemented by extensive regulations with wide ranging consequences for potential cases. Potential cases require historic information to be available and over the years the time over which cases can emerge has increased. This means any relevant information such as training, policies, incident details could be required and therefore should be retained for longer, often till age 100 or for 100 years.

2 Version Control and metadata

Where information is subject to revision and evidence of the history of the document is required, consistent version control procedures must be applied. This will ensure:-

- the reason for and authorisation of any amendments is evidenced,
- earlier versions can be preserved if required,

- out of date versions are clearly identifiable, avoiding confusion and improving storage.

This may be operated via specific IT systems or may be a defined consistent manual process.

Manual version control

Generally manual version control uses sequential numbers as the versions change. The version must be on the document (eg in the footer or at the front of the document) and within the file name.

- Before publication documents are labelled as “draft”, and may also have a date or sub version number to track amendments.
- When published the document is given the number 1.
- Subversions are labelled as 1.1, 1.2 etc.
- Any major revision is re-published as number 2 and so on.

Example:

Retention schedule draft	(- *awaiting approval)*
Retention schedule v1	(- approved and published)
Retention schedule v1.1	(- minor amendments)
Retention schedule v2.0	(- major changes or formally approved)

- Password protection or access restrictions can be used if changes must be prevented.
- Older versions could be moved to an archive folder to reduce possible confusion or maintain an audit trail of changes.
- Older versions of documents should only be deleted if no longer required, and in line with the retention schedule after noting the disposal details.

Metadata

In addition to version control information systems may require metadata to be completed in order to create an audit trail or facilitate searching. This may include:

- Author/creator
- Title
- Subject & keywords (those which would help searching)
- Description
- Date of creation & (if necessary) evidence of approval or authenticity
- Context if required to interpret information properly
- Version
- Security Marking (where appropriate)

Naming conventions

Information must be named consistently, using descriptions that other people will understand – ie using the authors name or a generic term such as “report” is not sufficient to clearly identify Service information.

3 RETENTION SCHEDULE

Asset acquisition and disposal	Under £50k – 6 years, over £50k – 12 years
Corporate annual reports	Permanently
Audit reports, plans Internal audits	6 years or permanently if historical interest 3 years minimum
Authorised signatories	Current year plus 6
Authority and committee meetings, agenda's, papers, minutes CFA recordings - in case of challenge to published minutes	Permanently 6 months or a full meeting cycle. Monitoring Officer may extend for 2 year review period.
BA records	40 years from last action for Health and Safety reasons
CCTV – buildings Fire appliances Command unit, body worn camera	1 month plus current month unless required for investigation or legal proceedings. Automatically overwritten, unless downloaded for investigation or legal proceedings - then held with incident for minimum 7 years Minimum of 7 years, extended depending on incident
COMAH	5 years
Community Safety campaigns and advice	3 years, or permanent if significant
Compliments and Complaints	10 years
Consultants reports	2 years unless required for evidence purposes
Contingency and Emergency plans	Minimum 5 years – permanently if utilised
Contracts and related records	7 years after expiry, 12 years if under seal
Control voice recordings Incident records (eg BOSS)	Held by NWFC - minimum 6 years, unless required locally for investigation or proceedings. Permanent, offer to Public Records after 7 years
Corporate Communications; Internal External Media cuttings	Generally - 1 year, 2 if signed 3 years 5 years
Corporate plans, IRMP, Business Continuity Tests Corporate Governance, Business Continuity Plan, Action plans, Audits, PDG plans etc	10 years from publication 5 years from publication
Correspondence - general Legal and important matters	2 years Permanently
Data Protection requests Disclosure made in respect of "Rights"	2 years from disclosure or from completion of any appeal, local or ICO. Then review and consider whether case may still be required.
Disciplinary warnings **NB** – Separate register kept in order to manage good service awards Disciplinary cases and dismissal	Unfounded (retain summary or finding only), IRD's, oral, written and final warnings – generally 5 years 7 years, provided no further concerns arise. **NB** Permanent for safeguarding/child protection matters
Employment applications for unsuccessful candidates, other interview records	1 year
Expense analyses/expense claims and records	7 years
Equal opportunities monitoring and impact	Current year plus 3

assessments	
Equipment records, maintenance and testing including, ICT, vehicles	7 years Note 40 years minimum for BA records
Finance Accounts payable ledgers and schedules Transactions (receipts, invoices, allowances, write-offs, cashbooks, vouchers, petty cash) Bank statements Capital budget and financing Cheques (for important payments/purchases) Bank reconciliations Year end financial statements	 7 years Current year plus 6 3 years Current year plus 6 Permanently 2 years Permanently
Fire Authority meeting recordings – in case of challenge to published minutes	6 months or a full meeting cycle. Monitoring Officer may extend for 2 year review period.
Fire investigations	15 years after last action Permanent for all fatalities and "unknown", and fires of Special Interest
Fire and incident reports (eg FDR1/IRS, debriefs), station handovers	7 years – permanently if historical interest and offer to Public Record Office
Fire Safety records, Prohibition Notices, Prosecution files SAFFIRE risk management information Alterations notice Notification of Fire Safety deficiency form Fire engineered solutions in premises Primary Authority advice	7 years from last action 7 years from the date the notice ceases 7 years after prosecution 7 years after closed 7 years from the date the notice ceases 7 years aligned with fire safety records Duration of the engineered solution Permanently
Fitness testing	3 years – within OPA Basic details also held within Personnel file (see "Attendance, Health and Well being").
Freedom of Information	Case files – 3 years Procedures and statistics 10 years Access decisions – 10 years
Grants – applications, correspondence, plans and reviews	7 years after completion
Grievance and dignity at work	Formal – permanent for monitoring purposes Informal – during employment
Health and Safety – accident records, audits, risk assessments, committee minutes	Permanently, (except work place inspections - 3 years)
Historically important material including pictures and publications	Permanently
H.S.A depersonalized property data (SAFFIRE)	Permanently
H.S.A personal data	7 years. Option to extend Vulnerable cases and referrals if required on a case by case basis
ICT logs, requests, usage, Helpdesk. ICT back ups	Current year plus 2 Until superseded
ID card records	During employment plus 1 year
Insurance records, accident reports, claims, policies, etc	Permanently
Inventories of products, materials, and supplies	7 years
Invoices	7 years
Joint Consultation minutes, correspondence	Permanently
Leave cards	Keep for 3 years, if person leaves forward to HR
Legal matters, opinions and cases	7 years minimum after close of subject or case
Maternity/paternity pay and records	3 years after the financial year concerned
Medical assessments	To age 100

Memorandum of Understanding/legal agreements	Permanently
Officers notebooks	Permanently – forward to OPA Business Support Manager, refer to Investigation and Evidence Gathering Procedures Edocs 260.
Performance reports, assessments and statistics	External – permanent Internal 5 years from publication
<u>Personnel files</u> Employment matters (contracts, terms, recruitment, qualifications, references, training) Attendance, health and well being (commendation, recognition, star awards etc) Payroll, pensions, death benefit forms Conduct/performance Career development - promotions Security records Meetings	 until age 100 until age 100 Permanently 7 years from event closure, option to extend if serious or ongoing concerns. Permanent for safeguarding/child protection matters 7 years from event or permanent if salary change 10 years for employees, 5 years for leavers Defined by content - normally 7 years minimum.
Policies - significant Subsidiary policies and procedures	Permanent – retain versions for evidence, legal, historical reasons. 7 years after being superseded.
Petitions	Current + 6 years
Pism	Permanently
Projects	6 years after completion
Property occupancy	7 years after conclusion of transaction Property history -permanently
Procedures, SLA's, standards, guidance	Until superceded – also see Policies
Purchase orders and invoices	6 years after transaction concluded
Redundancy	12 years from date of redundancy
Retirement and pension records	Permanently
Rates and council tax records	7 years after last transaction
Registers	Statutory – generally permanently
Risk management strategy and registers	5 years from publication date
Rotas, Staffing, Station Duty logs	Permanently
Safe and Well – health related records	14 months from data capture, linked to reporting process
Senior management meetings, agendas, papers, minutes	Permanent or 7 years if not strategic eg reviewing compliance, planning preparation
SSRI and 72D including radiation records	Maintain significant versions, minimum 7 years
Tax returns and worksheets	Permanently
Tendering process Expression of interest Tender issue, returns, unsuccessful tenders	 – 2 years after contract is let – 1 year after start of contract
Timesheets	7 years
Youth work involving individual case support and services to young people/children	Until D.O.B plus 25 years or 10 years from last interaction whichever is longer
Training recordings/CCTV in OTG suite	Retain current and previous assessment, option to extend where there are concerns
Vehicle and fuel records, and journey logs	Until vehicle disposal + 2 years – kept with vehicle by Workshops

Lease vehicle records Fuel receipts	Until employee is removed from the scheme 2 complete years
Volunteer applications and interview records Volunteer personnel files (PRF)	12 months from the date of appointment or unsuccessful notification 7 years from the date the volunteering ceases or last contact. Option to extend retention where there is a business need.