Information Governance

RECORDS MANAGEMENT POLICY

About

This policy sets out the Service's expectations regarding the appropriate use and management of records in the Essex County Fire and Rescue Service.

This Policy should be read in conjunction with the Data Protection Policy and the ICT Acceptable Use Policy.

POLICY INFORMATION	
ORGANISATION	Essex Police, Fire and Crime Commissioner Fire and Rescue Authority "The Authority" is the Data Controller as defined in Chapter 2 of the Data Protection Act (2018) (DPA).
SCOPE OF POLICY	This policy applies to all employees and departments in the Essex Police, Fire and Crime Commissioner Fire and Rescue Authority (the Authority). This includes temporary staff, agency workers, volunteers and those on secondments. This policy expressly includes staff in the Service Head Quarters, stations, and workshops and to all employees working remotely.
POLICY OPERATIONAL DATE	
POLICY PREPARED BY	Information Governance Officer and the Information Governance Manager
DATE APPROVED BY INFORMATION GOVERNANCE (IG) BOARD	
POLICY REVIEW DATE	To be reviewed in December 2021

WHAT THIS POLICY COVERS AND THE PURPOSE OF THIS POLICY	This policy outlines responsibilities for management of information to support secure access and effective retention, destruction and preservation processes. This policy reflects the commitment of the "Authority" to maintaining the efficient management of records. This is necessary for the effective delivery of our services and to maintain good corporate memory. This policy also aims to support the Service in harnessing the benefits of effective records management. These include: • Ensuring that our information can be found and retrieved quickly and efficiently. • Complying with legal and regulatory requirements. • Reducing the risk of litigation, audit and government investigations. • Minimizing storage requirements and reducing cost. • Control and availability of valuable information assets. • Efficient use of staff time. • Actively supporting the day-to-day business that underpins the delivery of a high-quality service to the public. • Maintaining the integrity of our records • Monitoring and audit cycles. This policy also applies to records that third parties manage on behalf of the Authority. The policy has been endorsed by the Information Governance Board and is aligned with the Lord Chancellor's Code of Practice on the Management of Records issued under section 46 of the Freedom of Information Act 2000 (the code).
Responsibilities	
THE SENIOR INFORMATION RISK OWNER (SIRO)	The SIRO is responsible for ensuring Information Risk Policy is developed, implemented, reviewed and its effect monitored.
THE INFORMATION GOVERANCE (IG) BOARD	This body has the overall responsibility for ensuring that the organisation complies with its legal obligations with respect to records management and general Information Governance. The Authority will provide training or information to employees to help them understand their responsibilities when handling official records.

THE INFORMATION GOVERNANCE MANAGER **INFORMATION GOVERNANCE OFFICER**	The responsibilities of the Information Governance Manager includes: • Setting out an effective records management policy for the Authority • Briefing the Board on records management responsibilities • Reviewing and updating and related policies • Ensuring that training for relevant stakeholders takes place • Delegating day to day responsibilities for Information and Records management to information asset owners • Leading on audits and monitoring compliance with this policy The responsibilities of the Information Governance Officer include: • Implementing an effective records management for the Service • Putting in place a framework that helps to oversee the organisation's records from their creation, preservation and disposal in line with relevant legislation and policies • Managing relevant records management platform or software. • Implementing actions from audits
INFORMATION ASSET OWNERS	The responsibilities of the Information Asset Owners include: • Working with teams and all stakeholders to ensure that their departments collect, store/retain, move, access and delete records appropriately and securely in compliance with relevant legislation • Reviewing and updating Information Asset Registers • Co-ordination departmental information sharing • Working within the Service retention schedule to regularly review and update departmental records. If these are out of date or no longer required, the records should be deleted. • Regularly review information in line with Retention Guidelines to make best use of the available storage space. • Ensure that the facilities available for storing and managing information meet legal requirements and best practice. • Maintain a selection procedure for identifying, reviewing and managing records with historical value.

LINE MANAGERS	Line Managers in departments across the Authority are responsible for working closely with Information Asset Owners to ensure that employees are aware of and adhere to the principles in this policy and other related policies
THE CORPORATE COMMUNICATIONS MANAGER	The corporate communications manager or delegate is responsible for: • Publicising records management communications across the Authority. • Addressing queries from journalists or media outlets. • Wherever necessary, ensure that activities such as open days and other public facing activities abide by data protection and records management principles.
THE HEAD OF ICT AND THE INFORMATION SECURTIY MANAGER	The Information Security Manager or delegate is responsible for: • Ensuring that all systems, services and equipment used for storing data meet acceptable security standards. • Performing regular checks and scans to ensure security hardware and software is functioning properly • Evaluating the suitability and security of any third-party services that the Authority might be using to process personal data. For example, cloud computing services. • Providing and actively managing file stores that are secured to protect files that contain personal data through additional password protection. • Having a plan for resilient systems, backups, etc. to prevent the loss of records • Providing solutions that allow the secure exchange of files with external parties.

ALL EMPLOYEES AND VOLUNTEERS	In accordance with this policy, all staff are responsible for managing, storing appropriately and disposing of the information they create and receive as part of their normal daily business activities. Employees should keep all data secure by taking sensible precautions and following the guidelines below. • All information in any format which we hold as a record of our activity must be retained after 'closure' in line with the Service Retention Schedule • The information you manage is only known to an appropriate audience such as those that need the information for their work • Official information must not be stored on a personal drive or on equipment not provided by the Service • Data must not be disclosed informally either within the authority or externally. When access to confidential information is required, employees can request it from their line managers. In particular, strong passwords must be used and they should never be shared. • Report data breaches immediately it is detected or suspected • Employees should request help from their Information Asset Owner or the Information Governance Team if they are unsure of any aspect of this policy.
SECURITY AND ACCESSIBILITY	Records and information must be stored and handled following the requirements of the Government Security Classification System. https://www.gov.uk/government/publications/government-security-classifications All records must be traceable and retrievable. File movements and movements of data must be tracked, including for files migrated into or out of the department through machinery of government changes. Digital continuity must be considered for the systems and formats that are used to store digital records. All records must be supported by metadata that documents their authority, status, structure, and integrity to demonstrate their administrative context and relationship with other records.

Data Storage, Use, Accuracy, Retention and Destruction	
USE AND STORAGE OF RECORDS	• When information is stored on paper, it must be kept in a secure place where unauthorised people cannot see it. • When not required, the paper or files should be kept in a locked drawer or filling cabinet. • Staff must ensure that printouts are not left where unauthorised people could see them. • When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts. • Records should be protected by strong passwords that are changed regularly and never shared between employees. • Records should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services. • Copies of official records should not be saved on personal electronic devices • Technical details of electronic data storage can be found in the Information Security Policy.

DATA ACCURACY	In complying with the Data Accuracy Principle as seen in Section 38 of the Data Protection Act 2018 records processed in the Service must be accurate and kept up to date in all departments. In order to achieve this: • Records must be held in as few places as necessary. Staff must not create any unnecessary additional data sets. • Information from third parties must be verified before using it on behalf of the Authority. • Records should be updated as soon as inaccuracies are discovered. • The Authority must make it easy for employees to update their personal information.
RETENTION PERIODS	In complying with the Storage Limitation principle as provided for in section 39 (1) of the DPA 2018, personal data must not be stored for periods longer than necessary. Full retention times for data held by various departments can be found in the Service Retention Schedule and Guidelines Records must only be retained beyond the stipulated ECFRS retention period if their retention can be justified for statutory, regulatory, and legal or security reasons or for their historic value. The Information Governance team must be notified of any record processing that is outside the set retention times.
LINE OF BUSINESS RETENTION AND DISPOSAL RESPONSIBILITIES	Records relating to pending audits, litigation or investigations must not be destroyed. Relevant records must be securely destroyed Processes must be in place to ensure that all backups and copies are included in the destruction of records, or that data is put beyond use.

MONITORING COMPLIANCE AND EFFECTIVENESS.	Information Asset Owners will have direct responsibility for ensuring their information practices are audited with support from Information Governance team. Where non-compliance or improvements could be made then these shall be agreed with process owners / managers and subsequently followed up. Failure to comply with this policy may result in ineffective working and an inability to meet the requirements of the Freedom of Information Act 2000 and the Data Protection Act 2018
DATA DESTRUCTION	Hard copies that are no longer required must be disposed of securely using the confidential waste bins or shredded securely. This also applies to digital copies in disks and other portable devices
REFERENCES AND ASSOCIATED DOCUMENTS/LEGISLATION	• Data Protection Policy • Retention Schedule • Information Security Policy • Acceptable use policy • Information Commissioners Office website https://ico.org.uk/ • National Archives (Public Records) https://www.nationalarchives.gov.uk/ • Government Security Classifications https://www.gov.uk/government/publications/government-security-classifications • Statutory request policy The Authority is obliged to meet the legal requirements for the retention and disposal of records in accordance with relevant legislation, particularly the Public Records Act 1958 (PRA 1958), the Freedom of Information Act 2000 (FOIA 2000) and the Data Protection Act 2018 (DPA 2018).

Right of Access to the records the Authority holds	
RESPONSIBILITY	The Information Officers in the Data and Performance Team are responsible for ensuring that the right of access requests are handled within the legal time limit. Managers and teams that hold information on requests from data subjects must prioritise these statutory request to avoid breach of relevant statutory provisions. This means passing on any information that might be required by a Subject Access Request to the Information Officers without delay.
PROVISION FOR VERIFYING IDENTITY	Where the person managing the access procedure does not know the individual personally there should be provision for checking their identity before handing over any information that contains personal data
CHARGING	Information will be provided free of charge to requesters. However, The Authority is able to charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. This will be in line with the Service Charging Schedule

PROCEDURE FOR STAFF SIGNIFYING ACCEPTANCE OF POLICY	Current employees are required to read, sign and return this policy to indicate their acceptance of their responsibilities to properly manage the records that they come across in their roles. This policy will form part of the contract of new employees.

ENFORCEMENT	After undergoing the necessary training and awareness sessions that are required for your role, deliberately or negligently breaching this policy may lead to disciplinary actions depending on the case.

Policy review	
RESPONSIBILITY	The responsibility for undertaking a review of this policy lies with the Information Governance Manager
PROCEDURE	In reviewing this policy, the SIRO, Information Asset Owners, the Information Governance Board, ICT Department, Corporate Communications and other relevant stakeholders at the time will be consulted.
TIMING	This policy will be reviewed in December 2021

Audit Trail

Page/para nos.	Brief description of change	Issue Date	Version Control