Information Governance

DATA PROTECTION POLICY

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 of 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	July 2018.
POLICY PREPARED BY	The Data Protection Officer.
DATE APPROVED BY INFORMATION GOVERNANCE (IG) BOARD	18th July 2018
POLICY REVIEW DATE	To be reviewed in June 2023

WHAT THIS POLICY COVERS AND THE PURPOSE OF THIS POLICY	"The Authority" controls both personal data and sensitive personal data as defined in Chapters 1 and 2 of the DPA 2018. These include names, addresses, date of birth, national insurance numbers, and occupational health records of data subjects. These category of personal data is the focus of this data protection policy. "The Authority" expects this policy and the good practice that it advocates to apply to all data, even if it is outside of the current data protection legislation. The main purpose of this policy is to implement the rights of data subjects (living individuals) as enshrined in Chapter 3 of the Data Protection Act 2018. These are: • The right to be informed • The right of access • The right to rectification • The right to erasure • The right to restrict processing • The right to data portability • The right to object • Rights in relation to automated decision making Abiding by these rights helps the Authority to achieve the following: • protecting staff, members of the public and clients • complying with the law • following good practice • protecting "the Authority" from reputational damage • Making staff aware of their rights and responsibilities under data protection legislation By working within this data protection policy, "The Authority" will mitigate the risk of non-compliance with data protection legislation and the associated impacts which include: • Reputational damage to the Authority • Financial losses arising from fines from the ICO • Compensation claims from individuals that their data have been breached. • Adverse impact on service delivery as a consequence of a data breach. The Authority is committed to informing Data Subjects on why and how their data is being processed as seen in the various privacy notices across the organisation.

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 data protection and general Information Governance.
DATA PROTECTION OFFICER	The responsibilities of the Data Protection Officer includes: • Briefing the Board on Data Protection responsibilities • Reviewing and updating Data Protection and related policies • Advising other staff on tricky Data Protection issues • Ensuring that Data Protection induction and training for relevant stakeholders takes place • Notification to the ICO • Advising on unusual or controversial disclosures of personal data • Advising on contracts with Data Processors
INFORMATION ASSET OWNERS	Information Asset Owners are key personnel that are responsible for overseeing how personal data is processed within their departments. Working with relevant stakeholders, they ensure that their departments collect, store/retain, move, access and delete personal data appropriately and securely. They must work with line managers to ensure compliance with data protection legislation.
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 carry out data protection obligations specific to their roles. They must ensure that the necessary training and awareness is provided and staff know how to report data breaches and incidents in a timely fashion.

THE CORPORATE COMMUNICATIONS MANAGER	The corporate communications manager or delegate is responsible for: • Publicising data protection statements and communications across the Authority. • Addressing data protection queries from journalists or media outlets. • Wherever necessary, ensure that activities such as open days and other public facing activities abide by data protection principles.
THE HEAD OF ICT AND THE INFORMATION SECURTIY MANAGER	The Information Security Manager or delegate are 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. • Work on projects to consider appropriate controls that prevent data loss. For example, encryption of disks of the MDTs or Tablet PC. • Providing solutions that allow the secure exchange of files with external parties. • Having a plan for resilient systems, backups, etc. to prevent data breach.

ALL EMPLOYEES AND VOLUNTEERS	• Employees should keep all data secure by taking sensible precautions and following the guidelines below. • The only people able to access data covered by this policy should be those who **need it for their work**. • Data **must not be shared informally**. When access to confidential information is required, employees can request it from their line managers. • The Authority will provide training to all employees to help them understand their responsibilities when handling data. • In particular, **strong passwords must be used** and they should never be shared. • Personal data **should not be disclosed** to unauthorised people either within the Authority or externally • Personal data should be **regularly reviewed and updated** if it is found to be out of data or no longer required, it should be deleted or securely disposed of. • Employees **should request help** from their Information Asset Owner or the Data Protection Officer if they are unsure about any aspect of data protection • Reporting breaches of personal data immediately it is detected or suspected.
SECURITY	The greater the consequence of a data breach, the tighter the security should be. Details of data security for the organisation are contained in the Information Security Policy. The Information Security Policy sets out the confidentiality level for various data and the security measures to be followed in compliance with Section 40 of the Data Protection Act 2018.

Data storage, use, accuracy, retention and destruction	
DATA STORAGE	When data 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, like on a printer When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts: • Data should be protected by strong passwords that are changed regularly and never shared between employees. • Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services. Technical details of electronic data storage can be found in the Information Security Policy.
DATA USE	• When working with personal data, staff must ensure that the screens of their computers are always locked when left unattended. • Personal data must not be shared informally. • Personal data must not be transferred outside of the European Economic Area without consultation with the Data Protection Officer and the ICT Manager. • Employees should not save copies of official personal data to their personal computers.

DATA ACCURACY	In complying with the Data Accuracy Principle as seen in Section 38 of the Data Protection Act 2018, personal data that is processed in the Service must be accurate and kept up to date in all departments: • Data must be held in as few places as necessary. Staff must not create any unnecessary additional data sets. • Staff should take every opportunity to ensure data is updated. For instance, where information is taken over the phone, this should be checked back with the individual. Information from third parties must be verified before using it on behalf of the Authority. • Data 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.
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.

Right of Access	
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.
DISCLOSING DATA FOR OTHER REASONS	Under specific circumstances, the Data Protection Act (2018) allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, The Authority will disclose requested data. However, The Authority will ensure that the request is legitimate, seeking assistance from the IG Board and from the legal team where necessary.

Reporting Data Breaches	
DUTY TO HANDLE BREACHES, WHAT TO DO IN THE EVENT OF A DATA BREACH OR INCIDENCE	The Data Protection Act 2018 places a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. This must be done within 72 hours of becoming aware of the breach, where feasible. Whenever there has been a personal data breach or incidence, it must be reported immediately by the employee or volunteer that comes across it using the online form on the intranet, the short cut on your desktop or by emailing databreach@essex-fire.gov.uk The completed form is provided to our Data Protection Officer who will determine whether it needs to be reported to the Information Commissioners Office (ICO). A record of all data breaches or incidents are kept by the Service.

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.

Lawful Basis	
	The legal basis for processing data in Authority is found in Chapters 2 3 and Schedules 1, 2 and 3 of the Data Protection Act 2018. These include: task carried out in public interest – promotion of fire safety, tasks carried out as part of a contract (HR) and activities being undertaken as part of performing a legal obligation such as the Regulatory Reform (Fire Safety) Order 2005 In the circumstances under which consent forms the lawful basis for processing personal data, this must be freely given, specific, informed and unambiguous. Data subjects must also be free to with draw their consent at any time. Full detail of the lawful basis for processing data in the Authority are recorded and fully documented in the document titled “Lawful Basis for Processing Data”.

Employee training & Acceptance of responsibilities	
INDUCTION	All new employees of the Authority are undertake a mandatory induction that includes what is expected of them with respect to personal data handling and security.
CONTINUING TRAINING	All employees must undertake the Authority's mandatory e-learning module on data protection. Additional data training is offered to employees that undertake Data Protection Impact Assessments (DPIAs) and those that handle contracts and suppliers on behalf of the Authority. Members of the Senior Leadership Team (SLT) are also required to undertake tailored data protection training to fully understand the responsibilities of data controllers and processors.
PROCEDURE FOR STAFF SIGNIFYING ACCEPTANCE OF POLICY AND CONSEQUENCES OF NON COMPLIANCE	Current employees are required to read, sign and return this policy to indicate their acceptance of their responsibilities to protect data that they come across in their roles. This policy will form part of the contract of new employees. Non compliance with this policy may result in disciplinary action.

Policy review	
RESPONSIBILITY	The responsibility for undertaking a review of this policy lies with the Data Protection Officer
PROCEDURE	In reviewing this policy, the SIRO, Information Asset Owners, the IG Board, ICT Department, Corporate Communications and other relevant stakeholders at the time will be consulted.
TIMING	This policy will be reviewed in June 2023