SAFER PEOPLE SAFER PLACES

LEICESTERSHIRE FIRE and RESCUE SERVICE

leics-fire.gov.uk

SERVICE POLICY
Personal Data Policy

Document History

Responsible Department
Information Governance

Version No. 4

Created	2007
Last Review	Jan 2023
Next Review	Jan 2025

disability confident COMMITTED

INTRODUCTION

This policy explains our commitment in aiming to comply with all the relevant legislation associated with personal data processing. Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is used:

- Fairly;
- Lawfully; and
- Transparently.

We are a Data Controller as defined in the Data Protection Act 2018. This means we determine what, why and how personal data and special category (sensitive) personal data is processed.

Personal data only includes information relating to natural living persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

Personal data may also include special categories of personal data, health data or criminal conviction and offences data. These are considered to be more sensitive and may only be processed in more limited circumstances.

Any actions leading to a breach of this policy, or failure to report a breach, will be investigated and may be subject to disciplinary procedures and criminal investigation.

KEY INFORMATION

2.1 Policy Statement(s)

2.1.1 We will appoint a Data Protection Officer (DPO) and register their contact details with the Information Commissioners Office (ICO), the United Kingdom Supervisory Authority (regulatory body).

2.1.2 We will register our Service annually with the ICO, listing the activities we carry out that involve processing personal data and paying the required fee.

2.1.3 We will assign Information Asset Owners (IAOs) to our personal data processing activities who aim to maintain an accurate and up-to-date Corporate Register Of Processing Activity (ROPA).

2.1.4 We aim to have appropriate technical measures in place to keep our personal data safe, secure and preventing unauthorised access.

2.1.5 For any personal data we obtain we aim to;

- only capture, record, store, use or share when we need to;
- collect the minimum required to perform our work;
- ensure it is accurate and up-to-date;
- only keep it for as long as we need to and then safely and securely dispose of it as soon as possible;
- only store it inside the European Economic Area or the United States of America. We aim to only store personal data outside of these areas if we are assured that the data will be adequately secured; and
- inform those people we collect data from of their rights.

2.1.6 We aim to be open and honest with individuals whose data is processed (the Data Subject) and tell them what we are doing with their personal data.

2.1.7 We will consider any request received from individuals to stop processing their data and where we can, we aim to comply and delete it.

2.1.8 We aim to have organisational measures in place including accountability and be able to show that our processing of requests for personal information from employees and non-employees is in accordance with the relevant Regulations, Statute and best practice.

2.1.9 We aim to comply with all requests for disclosure of personal data to our staff or non-employees;

- when we have a fair and lawful reason to do so;
- unless a lawful exemption from disclosure applies;
- identifying and sourcing the information that has been requested no matter how hard it is to find;
- explaining why we are not able to provide information when we cannot; and
- charging appropriate fees for the provision of personal information when we are entitled to do so.

2.1.10 We will have contracts in place with people and organisations who process personal data on our behalf (Data Processors).

2.1.11 We aim to have robust data processes, procedures and guidance for our staff to follow, ensuring that suitable training is

delivered to anyone accessing our personal data; we aim to record all formal data protection training carried out.

2.1.12 We will carry out Data Protection Impact Assessment's (DPIA's) to identify our privacy risks and consider 'privacy by design' features in new systems and software we may buy.

2.1.13 We aim to apply data protection requirements when we purchase or introduce new technology, or when we amend or introduce new procedures.

2.1.14 We aim to avoid the use of paper systems, but when we do have to use them, we aim to keep the documents safe and secure and transfer them to electronic format when we can, or dispose of them completely.

2.1.15 We aim to reduce and prevent any personal data breaches occurring; when they do we will investigate thoroughly and take any steps necessary to minimise the impact on people and the Service. Reporting them as and when required by legislation.

2.1.16 We aim to meet statutory time periods for all activities involving personal data processing, including ICO requirements.

2.1.17 We will have an internal review and complaints process should any person not be happy with the way their personal data or sensitive personal data has been processed, and we will inform people of their right to complain.

2.2 Scope

2.2.1 **All Employees of the Service**

You have a duty to:

- Be aware of relevant legislation;
- Ensure you understand and comply with your responsibilities within required timeframes; and
- Act fairly and lawfully when processing personal information including sharing with others.

2.2.2 **Information Governance Manager (Data Protection Officer)**

The Information Governance Manager is our appointed Data Protection Officer, with responsibility for ensuring that where we can, we comply with relevant legislation. They aim to do this by performing an advisory and monitoring role, and by overseeing the implementation of measures to support this policy.

2.2.3 **Information Governance Officer (Deputy Data Protection Officer)**
The Information Governance Officer supports the Information Governance Manager in the implementation of our measures in relation to compliance with this policy.

2.2.4 **Information & Communication Technology (ICT) Manager**
The ICT Manager is responsible for general ICT systems access and physical information security (technical measures).

2.2.5 **Assistant Chief Fire and Rescue Officer (Service Support) (ACFO)**
The ACFO (Service Support) is the Senior Information Risk Owner (SIRO). The SIRO is accountable and responsible for information risk across the Service.

2.2.6 **Chief Fire and Rescue Officer (CFO)**
The CFO is ultimately responsible for non-compliance with relevant legislation and is accountable to the Information Commissioner (Head of the Information Commissioners Office [ICO] that is the Supervisory Authority for the United Kingdom)

2.3 Name of Directly Supporting Procedural document(s)

Document Name	*Version*	*Date Published*	*Department*
Access to Personal Data	V1	01/09/2018	Information Governance
Memorandum of Understanding	V2	20/12/2013	Service Assurance
Partnerships	V2	26/11/2012	Service Assurance
Data Protection Impact Assessment DPIA	V2	01/09/2018	Information Governance

FURTHER INFORMATION

3.1 Impacted Policies

Policy Name	*Version*	*Date Published*	*Department*
ICT Protection of Information Policy	V1	7/12/2021	ICT

3.2 Other Impacted Procedure

Procedure Name	*Version*	*Date Published*	*Department*
All ICT system access and use procedures and guidance	Various	Various	ICT

3.3 Associated Non LFRS Documents

Documents	*Version*	*Date Published*
General Data Protection Regulation (GDPR)	2016/679	25/05/2018
Data Protection Act 2018	V1.0	25/05/2018
Human Rights Act 1998	V1.0	09/11/1998
Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (as amended)	V2.0	29/03/2019 [Latest]

Document History

This Version No.	4
Department Approver	Information Governance Manager / AM Service Assurance
Date Policy Officer Assessed	7/10/2020
Date SMT Approved	28/10/2020
Date SCF Approved	4/2/2021
Impact Assessments Completed	Equalities Impact Assessment dated
Review Year	2 year (original 1yr changed to 2yrs at 2023 review)

Date of Publication	Version No.	Brief Details of Alterations	Dept Owner	Approved By
April 2007	1	Original Data Protection document produced	Data Management	SMT
March 2019	2	Replaces Data Protection Procedure dated April 2007	Information Governance	SMT
February 2020	3	Revised and transferred to new template	Information Governance	SMT
March 2022	4	Following review only revision of 2.1.3 to update terminology. Meaning of statement unchanged.	Information Governance	N/A
February 2023	4	No Changes following review	Information Governance	N/A