SUMMARY COVER SHEET – Data Protection

DEVON & SOMERSET FIRE & RESCUE SERVICE

Information Assurance Service Policy Document

Target Audience

This document is intended for all staff and third parties who deal with DSFRS personal information assets.

Version Control

Version	Date	Details
0.1	Apr 2018	Initial
0.3	May 2018	Includes requirements of final DPA 2018

Summary of Main Changes:-

Revised to include changes from the UK Data Protection Act 2018 / GDPR

DEVON & SOMERSET FIRE & RESCUE SERVICE

Information Assurance Service Policy Document

Document Purpose:-

Policy for the protection and security of Devon and Somerset Fire & Rescue Service (DSFRS) personal information assets.

NOTE – If you are reading a paper copy of this document it may not be the most up to date version. For the latest version view the information on the Service Intranet.

Document Status:-

Ownership:	Information Assurance Manager / Data Protection Officer (DPO)
Date first Published:	09/02/2010
Review Date:	Every 2 Years
Last Review or Amendment:	09/06/2018
Key Consultees:	SIRO, Information Asset Owners,

Further Information:-

- Information Security Policy
- IT Security Policy
- Social Media Policy
- Information Asset Register & Record of Processing Activity
- Reporting Information Security Event Procedural Guidance

Cross-References:-

- The General Data Protection Regulation (GDPR)
- The UK Data Protection Bill / Data Protection Act 2018
- The Information Commissioners Office
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act
- Environmental Information Regulations
- The National Archives

POLICY STATEMENT

The purpose of this policy is to ensure that DSFRS has robust procedures in place for demonstrable compliance with the Data Protection Laws.

DSFRS is committed to protecting the personal data it holds relating to staff and members of the public, ensuring it is used appropriately to comply with the General Data Protection Regulation and the Data Protection Act 2018 (hereafter DP Laws).

Malicious or negligent failure to comply with this policy may constitute a disciplinary matter.

COMPLIANCE STATEMENT

The Service will not unlawfully discriminate against any persons in the application of this policy or any subordinate procedures and will use any opportunities it presents to further our positive duties under the Public Sector Equality Duty 2011.

To this end, this policy has undergone consideration against the requirements of an Equality Risks and Benefits Assessment and no significant risks to any protected characteristic were identified. The consideration of an ERBA is due for review at the same time as the policy.

This policy is open under the Freedom of Information Act 2000.

KEY INFORMATION

- The Data Protection Act 2018 includes principles which data users must comply.
- Whenever DSFRS works with personal data it will be:

a)processed fairly, lawfully and transparently (see DSFRS Privacy Notices and Records of Data Processing)

b)collected for specific purposes and not used for incompatible purposes

c)adequate, relevant and limited to what is necessary

d)accurate and, where necessary, kept up to date

e)retained no longer than necessary (see DSFRS Records Retention Schedule)

f)kept securely (see DSFRS Information Security Policy)

- The principles apply to "personal data" - ***any*** information from which an individual is identifiable (directly or indirectly).
- Special category personal data requires an additional lawful condition to be met.
- The Data Protection Officer (DPO) is the statutory compliance officer who: advises DSFRS, the SIRO, Protective Security Group (PSG) and Information Asset Owners on their compliance with DP Laws.
- The Director of Corporate Services as **Senior Information Risk Owner** (SIRO) is the senior corporate lead for data protection, providing strategic direction for the service's compliance activities and ensuring Executive Board gives appropriate consideration to data protection issues in their decision making.
- **Information Asset Owners** (IAOs) are responsible for: providing assurance to the SIRO and PSG that the personal data assets they are accountable for have appropriate controls in place.
- Up to date Privacy Notices will be maintained by the DPO by Information Asset Owners providing updates on changes to processing activity within their areas of responsibility.
- An **Information Asset Register** and **Record of Processing Activities** describing the content, purpose, controls and the DSFRS IAO with accountability for each data system or set of records holding personal data will be maintained. In compliance with DPA 2018, Schedule1, section 41 the Record of Processing Activities will include clear explanation of the processing condition and lawfulness of processing of special category personal data and criminal personal data. It will also record the retention periods identified for and applied to such data.
- A **Privacy By Design** culture will be followed through seeking the advice of the DPO on the acquisition and development of new information systems and on proposals for significant new business processes and change.

- DSFRS will ensure **individuals' rights** are respected with regard to their personal data.
- Any event which may **impact on the confidentiality, integrity or availability** of personal data held by DSFRS **must be reported immediately** to the DPO

CONTENTS

1. INTRODUCTION

DSFRS has a legal obligation to manage its personal data in accordance with the Data Protection Act 2018 and General Data Protection Regulation (the Data Protection laws).

Changes to data protection legislation came into force on the 25th May 2018.

This policy document applies in particular to special category personal data and criminal personal data processed by DSFRS to meet out obligations under employment law, to meet our obligations for measuring and promoting equality, or as necessary in the substantial interest to perform our statutory obligations of fire prevention and investigation. This policy document will be kept current and made available on request to the Information Commissioner, in compliance with sections 39 and 40 of Schedule 1 of the DPA 2018.

2. LEGISLATION AND GUIDANCE DOCUMENTS

Data Protection Act 2018 (DPA)
General Data Protection Regulation (GDPR)
Computer Misuse Act
Freedom of Information Act (FOI)
HMG Security Policy Framework (SPF)
ISO27001
IT Password Guide
IT Acceptable Usage Guide

3. DSFRS Roles and Responsibilities

- The Director of Corporate Services as **Senior Information Risk Owner** (SIRO) is the senior corporate lead for data protection, providing strategic direction for the service's compliance activities and ensuring Executive Board gives appropriate consideration to data protection issues in their decision making.

  The SIRO also decides on behalf of DSFRS, and on advice from the DPO, whether personal data breaches by DSFRS merit being reported to the ICO.

- The **Protective Security Group** (PSG) The Protective Security group (PSG) provides strategic oversight of data protection compliance, including reviewing trends in data events and audit reports with a view to identifying and driving improvements, and considering any Data Protection Impact Assessments where significant risks cannot be mitigated.

- The **Data Protection Officer (DPO)** is the statutory compliance officer who: advises DSFRS, the SIRO, PSG and Information Asset Owners on their compliance with DP Laws; takes appropriate steps to monitor compliance across DSFRS; receives reports of personal data events and breaches and advises SIRO on reporting breaches to the ICO; advises Information Asset Owners on the completion of Data Protection Impact Assessments; response to queries related to data protection from DSFRS staff and the public; ensures data subjects rights requests are dealt with appropriately and in a timely manner; ensures the provision of appropriate data protection training and awareness to DSFRS staff; maintains the core corporate DSFRS Privacy Notice; holds the DSFRS Information Asset Register and Record of Processing Activities. This role is incorporated into the Information Assurance Manager role and is supported by the Information Assurance Team.

- **Information Asset Owners** (IAOs) are responsible for: providing assurance to the SIRO and PSG that the personal data assets they are accountable for have appropriate controls in place for access, security, retention, accuracy and data minimisation; ensuring Data Protection Impact Assessments are conducted as appropriate on data processing activities in their business area, drawing on advice from the DPO; ensuring the records for their business area on the DSFRS Information Asset Register and Record of Data Processing Activities are complete and current; ensuring appropriate and current specific Privacy Notices are provided as appropriate.

- **Line Managers** are responsible for ensuring that all staff complete appropriate data protection training (including all-DSFRS training and role- or function-specific training) and are aware of their responsibilities.

- **All DSFRS staff** are responsible for understanding and complying with DSFRS policies and procedures for handling personal data, appropriate to their role, and for immediately reporting any event or breach affecting personal data held by DSFRS via the ICT Service Desk or Fire Control (out of hrs). All staff are required to complete and regularly refresh on the Protecting Information Essentials or Protecting Information Briefing e-Learning course depending on their role.

4. Governance

DSFRS will maintain robust oversight and transparency in the management of personal data. We will meet our record-keeping duties through the maintenance of:

- Up-to-date **privacy notice information** (see article 13 and 14 of GDPR);
- An **Information Asset Register** and **Record of Processing Activities (ROPA)** describing the content, purpose, controls and the DSFRS IAO with accountability for each data system or set of records holding personal data;
- A **log of information security events**
- The **Protective Security Group** (PSG) who will provide operational oversight of data protection compliance.
- **The Information Security Forum** (ISF) who will embed a risk aware culture.

5. Privacy by Design

- DSFRS will apply **Privacy By Design** principles for new systems and business processes through seeking the advice of the DPO and from members of the Information Assurance Team on the acquisition and development of new information systems and on proposals for significant new business processes and change.

- DSFRS shall include privacy screening questions in the Strategic Change and Continuous Improvement processes to signpost colleagues to early engagement with the DPO as appropriate for new initiatives.

- The DPO shall have early visibility of senior management papers and agendas to allow identification of relevant points for intervention.

- As appropriate, the DPO may instruct the relevant Information Asset Owner to complete a Data Protection Impact Assessment in line with the DSFRS template and guidance from the ICO.

- All contracts with organisations who are processing personal data on behalf of DSFRS (**data processors**) will have GDPR-compliant contract clauses and be subject to appropriate levels of review and oversight. This will clearly set Service expectations in how 3rd party contractual suppliers must handle DSFRS personal data.

- DSFRS approved Information Sharing Agreements will be used when sharing personal information with non-contractual suppliers such as statutory and non-statutory partner organisations. All agreements must be reviewed by the DPO and signed on behalf of the Service by the SIRO.

6. Data Minimisation and Accuracy

- All DSFRS staff must only record appropriate, accurate and relevant personal data in the line of their DSFRS duties. This must be held on authorised DSFRS forms or information systems – not on unofficial notes or personal hard drives.

- IAOs will keep information systems, forms and templates under review to ensure that they are designed only to capture the minimum of personal data appropriate to the DSFRS business activity.

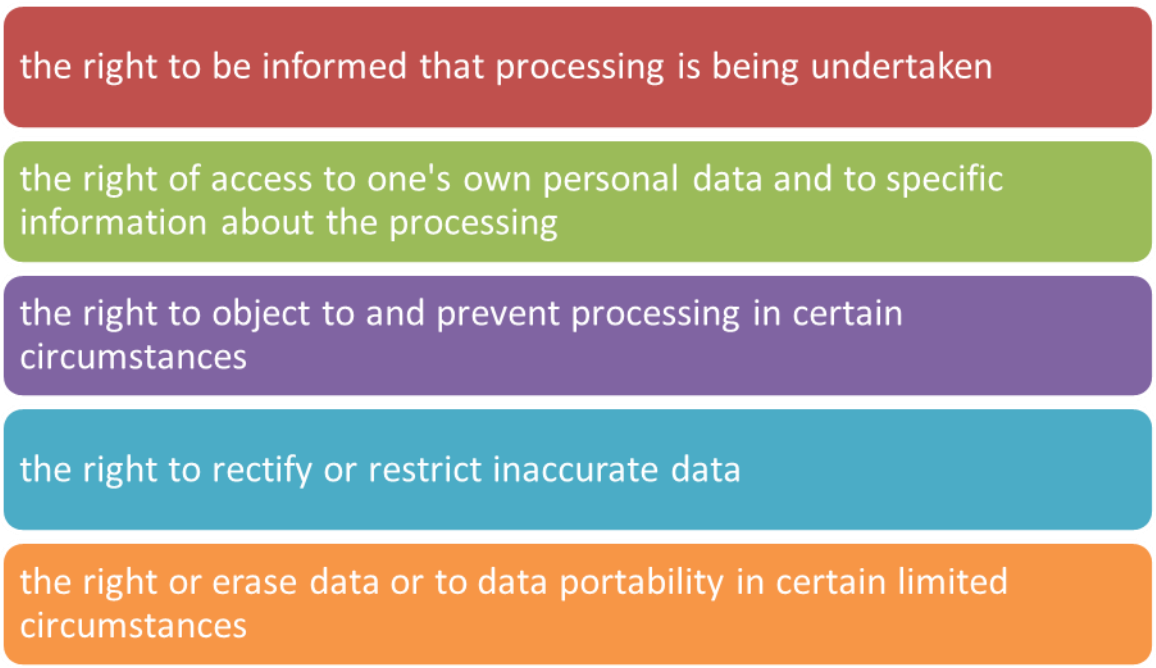
7. Retention of Data

- Personal data must not be retained for longer than is necessary. DSFRS Information Asset Owners and managers are responsible for ensuring that the Record Retention Schedule within the Information Asset Register is applied to all records and documents holding personal data, by having regular or automated deletion or destruction of personal data in systems, paper files and on network folders.

- All documents containing personal data should be disposed of securely using the Service's confidential waste procedure.

8. Individual Rights

- DSFRS will ensure individuals' rights are respected with regard to their personal data when applicable. These include:



- All requests relating to an individual's rights must be directed to the DPO or a member of the Information Assurance Team who will ensure that appropriate actions are taken, a response issued without undue delay and at least within one month.

9. Personal Data Events and Breaches

Any event which may impact on the confidentiality, integrity or availability of personal data held by DSFRS must be reported immediately to the DPO. This is reported via the ICT Service Desk during office hours or via Fire Control out of office hrs. Such events could include:

  - Loss of DSFRS records, laptops or media containing personal data;
  - Unauthorised access to DSFRS information systems containing personal data;
  - Access to personal data with no justifiable business need;
  - Personal data being misdirected to an incorrect recipient via email;

- All reported events will be recorded to ensure appropriate mitigation measures are in place and will consider whether the event meets the GDPR definition of a personal data breach which presents an adverse impact to individuals.
- The DPO will present a report to the SIRO including, if appropriate, a recommendation on whether to report a breach to the Information Commissioner's Office within 72 hours of DSFRS becoming aware of the event.
- If the SIRO decides that an incident constitutes a reportable breach, the DPO will report the incident to the ICO and liaise as appropriate.
- If a data breach causes an adverse impact to an individual, the DPO will notify the data subject of the event.
- All reported events will be analysed to identify trends and target areas for improvement.
- A record will be kept of the cause of the event including the person responsible. A trigger system based on significance and the number of events will be used to determine appropriate outcomes for repeat occurrences. More information can be found in the procedural guidance for Reporting Information Security Events.