Policy – Data Protection

Policy owner: Information Governance

This policy applies to the following members of staff:

All staff

Responsible staff must ensure that any visitors or those with remote access to the Service's sites (guests, contractors, temporary staff etc.) are aware that this policy also applies to them.

Policy purpose

The purpose of this policy is to ensure that DSFRS has robust procedures in place for demonstrable compliance with 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 (GDPR) and the Data Protection Act 2018 (hereafter Data Protection Legislation).

This policy explains what we will do as an organisation, who it applies to and why.

Statements of intent

The Service will comply with processing principles outlined in Data Protection legislation. Whenever Service personnel work with personal data it will be:

a. Processed fairly, lawfully and transparently
b. Collected for specific purposes and not used in an incompatible way
c. Adequate, relevant and limited to what is necessary
d. Accurate and kept up to date
e. Retained for no longer than is necessary
f. Kept securely

The principles apply to "personal data" - ***any*** information from which an individual is identifiable (directly or indirectly).

Key information

1. Roles and responsibilities

- The Director of Governance & Digital Services has the role of **Senior Information Risk Owner** (SIRO) and is the executive lead for data protection, providing strategic direction for the service's compliance activities and ensuring Executive Board considers data protection issues in their decision making. The SIRO is accountable for making an informed decision, and on advice from the Data Protection Officer (DPO), whether a personal data breach is reportable to the ICO.

- The **Protective Security Group** (PSG) provides strategic oversight of the Personal Information Management System 'control framework' and Service compliance.

- The **Data Protection Officer** (DPO) is the statutory compliance officer who: advises Service personnel, the SIRO, PSG members and Information Asset Owners on legislative compliance; takes appropriate steps to monitor compliance across the Service; receives reports of personal data events and breaches and advises the SIRO on reporting requirements to the ICO; advises Information Asset Owners on the completion of Data Protection Impact Assessments; responds to legislative queries from staff and the public; ensures an individual's rights to personal information is dealt with appropriately and in a timely manner; ensures the provision of appropriate training and awareness to staff; maintains an up to date corporate Privacy Notice and advises others on their responsibilities for transparency; holds the Service Information Asset Register (IAR) and Record of Processing Activities (ROPA). This role is incorporated into the Information Governance Manager role and is supported by the Information Governance Team.

- **Information Asset Owners** (IAOs) are responsible for: providing assurance to the SIRO (via the DPO) 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 (DPIAs) are conducted as appropriate on high risk data processing activities in their business area; drawing on advice from the DPO; ensuring the records for their business area are up to date on the Service IAR & ROPA; ensuring appropriate and current specific Privacy Notices are provided as appropriate.

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

- **All Personnel** 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.

2. Governance

The Service 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 (IAR)** and **Record of Processing Activities (ROPA)** describing the content, purpose, controls and the responsible 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 Governance Forum** (IGF) who will promote a data risk-aware culture.

3. Privacy by design

- The Service will apply **Privacy by Design** principles for new systems and business processes through seeking the advice of the DPO and Information Governance Team on the acquisition and development of new information systems and on proposals for significant new business processes and change.

- The Service shall include privacy screening questions in key organisational processes to signpost colleagues to early engagement with the DPO to inform decision making and achieve legislative compliance.

- As appropriate, the DPO may instruct the relevant IAO to complete a DPIA for any high-risk processing as determined from the privacy screening questions.

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

- 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.

4. Data minimisation and accuracy

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

- IAOs are accountable for ensuring information systems, forms and templates capture the minimum personal data as appropriate which is sufficient for the business activity.

5. Retention of data

- Personal data will not be retained for longer than is necessary. The Information Governance Team will work with IAOs and Information Asset Administrators (IAAs) to ensure the Record Retention Schedule within the legally required Record of Processing Activity (ROPA) is applied to all listed processing purposes.

- Personal data that is processed within newly developed 'in house' systems will have deletion or destruction built in to automatically manage the required retention schedule.

- Retention of data will be included in Privacy Notices and agreed with 3rd party processors in advance.

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

6. Individual's rights

- The Service will ensure individuals' rights are respected regarding their personal data when applicable. These include:

    - The right to be informed that processing is being undertaken
    - The right of access to one's own personal data and to specific information about the processing
    - The right to object to and prevent processing certain circumstances
    - The right to rectify or restrict inaccurate data
    - The right to erase data or port data in certain circumstances

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

7. Personal data events and breaches

- Any event which may impact on the confidentiality, integrity or availability of personal data held by the Service must be reported immediately.

- Event reporting must indicate if the Network Fire Services Partnership (NFSP) is implicated. The Information Governance Team must notify the affected partner organisation(s) immediately if NFSP is affected.

- 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 (ICO) 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.

- 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.

8. Processing special category and criminal offence personal data

- The Service will, as it is lawfully obliged, maintain an appropriate policy document specific to the processing purposes of special category and criminal offence data. This policy is called the 'Processing Special Category & Criminal Offence Personal Data Policy'.

- The Service will carry out a DPIA on any new processing of special category data to ensure the risk is necessary, proportionate and mitigated. Unmitigated high risk will be reported to the ICO by the DPO as required.

- The Service will identify and be transparent in their reliance on a 2nd lawful basis as per Article 9 of the GDPR wherever special category or criminal offence personal data is processed.

Monitoring and assurance

The author of this policy will:

- Maintain a Personal Information Management System (PIMS) to monitor compliance with this policy.
- Produce a regular compliance monitoring report to the SIRO and PSG.

Maintain an up-to-date baseline control set for the Personal Information Management System (PIMS) to provide assurance to the SIRO and Executive Board.