Staffordshire Fire and Rescue Service
preventing • protecting • responding

Appropriate Policy Document

Schedule 1, Part 4, Data Protection Act 2018

CONTENTS

1. INTRODUCTION

When processing personal data, Staffordshire Fire and Rescue Service will comply with the requirements of the EU General Data Protection Regulation 2016/679 (EU GDPR), the Data Protection Act 2018 (DPA) and any associated legislation.

The Data Protection Act 2018 provides for safeguards that must be implemented when processing special categories of personal data. This Appropriate Policy Document sets out the information required by Schedule 1 of the Data Protection Act 2018 when processing special categories of personal data in reliance on one of the conditions contained in that schedule.

This Appropriate Policy Document will cover all processing of sensitive personal data carried out by Staffordshire Fire and Rescue Service for which all of the following conditions are met:

- The data controller is processing personal data which is the subject of Articles 9 or 10 of EU GDPR.
- The data controller is processing this personal data in reliance of a condition listed in Parts 1, 2 or 3 of Schedule 1 of the DPA.
- The condition listed in Parts 1, 2 or 3 of Schedule 1 includes a requirement for the data controller to have an Appropriate Policy Document.

2. DEFINITIONS

Biometric data - personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a human being, which allow or confirm the unique identification of that person, such as facial images or fingerprints;

Consent of the data subject - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Controller - the person, company, public authority (i.e. SFRS), agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Data Protection Act – the current UK legislation governing data protection. This is currently the Data Protection Act 2018;
Data Subject – an individual who is the subject of personal data;

Filing system - any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

Genetic data - personal data relating to the inherited or acquired genetic characteristics of a human being which give unique information about the physiology or the health of that person and which result, in particular, from an analysis of a biological sample from the person in question;
Information Commissioner (ICO) – the UK's independent body responsible for monitoring the Data Protection Act, see www.ico.org.uk ;

Personal data - any information relating to an identified or identifiable human being ('data subject'). An identifiable human being is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (user ID or cookie) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that human being.

Personal data includes, but is not limited to, an individual's:

- Name
- Address
- Telephone numbers
- Identification numbers, such as Payroll number, Service number or National Insurance number
- Recordings, photographs or reproductions of a person's voice, likeness or image
- Bank account numbers
- Medical records, attendance and sickness records
- Online identifiers (e.g. username).

A person's favourite football team, job title, etc. are not typically personal data.

Special categories of personal data – this includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

Personal data breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Privacy – privacy can be defined in several ways, including 'the right to be left alone'. The term also covers freedom from unauthorised access to information deemed personal or confidential and freedom from being observed, monitored, or examined without consent or knowledge. Invasion of privacy can involve intrusion on a person's physical solitude or seclusion, public disclosure of private facts, publicly placing someone in a false light or appropriating a person's name or likeness for your own advantage (e.g. identity theft).

Processing - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Processor - a person, company, public authority, agency or other body which processes personal data on behalf of the controller;

Profiling - any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a human being, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Pseudonymisation - the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable human being;

Recipient - a person, company, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Restriction of processing - the marking of stored personal data with the aim of limiting their processing in the future;

Third party - a person, company, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

3. RELEVANT SCHEDULE 1 CONDITIONS AND DATA PROCESSING ACTIVITIES

Staffordshire Fire and Rescue Service may process special categories of personal data in reliance on the following Schedule 1 conditions. Examples of the types of personal data processed in connection with each condition are also listed:

Part 1 – Conditions Relating to Employment, Health and Research, etc.

- Employment, social security and social protection
  - Processing personal data concerning health in connection with the Service's rights under employment law and duties under the Health and Safety at Work Act 1974.
  - Processing data relating to criminal convictions under Article 10 EU GDPR in connection with the Service's rights under employment law in connection with recruitment, discipline or dismissal.
- Health or social care purposes
  - Providing human resources and occupational health facilities for employees in the assessment of the working capacity of an employee and the provision of reasonable adjustments and treatment.

Part 2 – Substantial Public Interest Conditions

- Statutory etc. and government purposes
  - Fulfilling the Service's obligations under the Fire and Rescue Services Act 2004 such as responding to emergencies and providing community safety advice.
  - Complying with other legal requirements, such as the requirement to disclose information in connection with legal proceedings.
- Equality of opportunity or treatment
  - Ensuring compliance with the Service's obligations under legislation such as the Equality Act 2010.
  - Ensuring that we fulfil our public sector equality duty when carrying out our work.
  - Ensuring we provide equal access to our services, to all sections of the community in recognition of our legal and ethical duty to represent and serve communities.
- Preventing or detecting unlawful acts
  - Processing data concerning criminal records in connection with employment in order to reduce the risk to the Service and the community.
  - Carrying out enforcement action in connection with the Service's statutory duties.

- Protecting the public against dishonesty etc.
  - Processing data concerning criminal records in connection with employment in order to protect the local community.
  - Carrying out enforcement action in connection with the Service's statutory duties.
  - Carrying out investigations and disciplinary actions relating to our employees.
- Regulatory requirements relating to unlawful acts and dishonesty etc.
  - Complying with the Service's enforcement obligations under the Regulatory Reform (Fire Safety) Order 2005.
  - Assisting other authorities in connection with their regulatory requirements.
- Preventing fraud
  - Disclosing personal data in accordance with arrangements made by an anti-fraud organisation.
- Safeguarding of children and individuals at risk
  - Carrying out community risk assessments in order to identify households for targeted fire prevention visits.
  - Identifying individuals at risk while attending emergency incidents.
  - Obtaining further support for children and individuals at risk by sharing information with relevant agencies. Where possible, consent will be sought, except when seeking that consent would not be reasonably expected or would put our employees at risk or the individual at risk of further harm.
- Safeguarding of economic well-being of certain individuals
  - Carrying out community risk assessments in order to identify households for targeted fire prevention visits.
  - Identifying individuals at risk while attending emergency incidents.
  - Data sharing with our partners to assist them to support individuals.
- Occupational pensions
  - Fulfilling the Service's obligation to provide an occupational pension scheme.
  - Determining benefits payable to dependents of pension scheme members.
- Disclosure to elected representatives
  - Assisting elected representatives such as local government Councillors and Members of Parliament with requests for assistance on behalf of their constituents.

Part 3 – Additional Conditions Relating to Criminal Convictions, etc.

- Extension of conditions in Part 2 of Schedule 1 referring to substantial public interest.
  - The Service may process personal data relating to criminal convictions in connection with its enforcement obligations or as part of recruitment and employment checks to protect the public against dishonesty.

4. PROCEDURES FOR SECURING COMPLIANCE WITH THE DATA PROTECTION PRINCIPLES CONTAINED IN ARTICLE 5 OF EU GDPR

In summary, Article 5 of the GDPR states that personal data shall be:

- processed lawfully, fairly and transparently
- collected for specific and legitimate purposes and processed in accordance with those purposes
- adequate, relevant and limited to what is necessary for the stated purposes
- accurate and, where necessary, kept up-to-date
- retained for no longer than necessary, and
- kept secure

In addition, Article 5 requires that the data controller shall be responsible for, and able to demonstrate compliance with, these principles (the accountability principle).

The Service's Data Protection Policy sets out requirements for the data protection principles to be complied with when processing personal data within the Service. The Service's Data Protection Officer ensures that the data protection principles are applied and that the Service can be held accountable for the personal data it processes.

When processing special category data, the following procedures are used to ensure compliance with the data protection principles:

- processed lawfully, fairly and transparently
  - Provision of privacy notices.
  - Compliance with conditions from both Article 6 and Article 9 of EU GDPR.
  - Use of data protection impact assessments to ensure proposed processing is carried out fairly.
- collected for specific and legitimate purposes and processed in accordance with those purposes
  - Privacy notices set out the purposes for which personal data will be used.
  - Personal data is not processed for other purposes without obtaining the data subject's consent unless authorised by law.
- adequate, relevant and limited to what is necessary for the stated purposes
  - Use of data protection impact assessments to ensure that collected data is sufficient to provide the service but not excessive in order to protect individuals from harm.
  - Use of national guidance and relevant legislation to determine information that we should collect.
- accurate and, where necessary, kept up-to-date
  - Cross-matching data sets where possible to check accuracy.

  - Review of personal information held when making contact with data subjects.
  - Correction of personal data when notified by data subjects exercising their rights in accordance with Article 16 of EU GDPR.
- retained for no longer than necessary
  - Retention periods are set out in the Service's information asset register and privacy notices.
  - Retention periods are based on legal requirements to retain data and consideration of the needs of data subjects through data protection impact assessments.
- kept secure
  - The Service adheres to the Government's Minimum Cyber Security Standard and implements information security controls in line with Cyber Essentials Plus and ISO 27001.
  - The Service's Protective Security Steering Group meets regularly to ensure suitable information security governance is employed within the Service.
  - All users of the Service's computer systems are vetted in line with HMG Baseline Personnel Security Standard.
  - Technical security controls such as encryption are employed to secure sensitive information within systems.
  - Role-based access controls are implemented to restrict access to sensitive data.
  - Where possible, anonymization or pseudonymisation are used to reduce the risk of sensitive data being compromised.

5. RETENTION AND ERASURE OF PERSONAL DATA

Personal data is held and disposed of in line with the Service's Record Retention and Disposal Policy. When disposing of information, the Service ensures this is carried out securely by using physical destruction methods as well as electronic data deletion.

The Service's Record of Processing Activities contains details of the retention periods for the Service's data processing activities together with information on the lawful basis for processing this data. If information is not retained or deleted in line with the policy then the reason is recorded in the Record of Processing Activities.

6. RESPONSIBILITY FOR PROCESSING SENSITIVE DATA

All employees are required to comply with the Service's Data Protection policies when processing personal data and to ensure that any processing of sensitive personal data is carried out legally, fairly and transparently. Information Asset Owners are responsible for ensuring that systems and processes under their control comply with current data protection legislation and that personal data is processed in accordance with the data protection principles.

The Protective Security Steering Group will review this Appropriate Policy Document annually to ensure that it remains current and relevant. Previous versions of this document will be retained for

at least six months after any specified processing of sensitive personal data referred to in that document have ceased. The Data Protection Officer is responsible for ensuring previous versions of this document are made available on request and for ensuring this document is reviewed and updated when necessary.

Date approved by Protective Security Steering Group:

Date for review: 22 August 2020