Data Protection Policy

This document is uncontrolled when printed. All users are responsible for checking the intranet to confirm that this is the current version before use.

Contents

1. Introduction

A range of legislation exists to protect personal data and ensure that organisations are transparent and accountable in the way that they deal with people's information. Avon Fire & Rescue Service (AF&RS) is trusted to handle personal and sensitive data and we must ensure that data protection is considered across the organisation and be able to demonstrate how we comply with the law.

This Policy is part of a suite of AF&RS Corporate Policies, which make up the Information Security Management System (ISMS).The following Policies may be read in conjunction for a fuller context about how we manage information and keep it safe.

- Information Security Policy*
- Freedom of Information Policy*
- Security Incident Management Policy
- IT Acceptable Use Policy
- Information Classification Policy

*These documents are available to staff and members of the public via the website.

2. Purpose

This Policy defines how AF&RS will adhere to Data Protection Legislation and ensure that all personal information that we hold, whether that is in relation to our staff, our community, our contractors, law enforcement agencies, our partners or our operational data, is fairly and lawfully processed.

3. Scope

This Policy applies to the entire scope of operation of AF&RS, regardless of how information is collected, recorded and used, and whether it is stored on paper, in computer records or recorded by any other means.

4. Definitions

Data Protection Legislation

A range of legislation exists to protect personal data, this will be referred to throughout this Policy as 'Data Protection Legislation'. The most relevant are listed here:

The EU **General Data Protection Regulation** (the GDPR) ensures fundamental data protection rights and freedoms for individuals, particularly the right to privacy.

It also places obligations on organisations to be accountable and transparent in the way that they use individuals' data. It aims to achieve consistency across all EU Member States, supports the free movement of trade and people, and reflects the changes in technology and more advanced data processing methods. The GDPR will still apply when the UK leaves the EU.

The **Data Protection Act 2018** (DPA) should be read alongside the GDPR for organisations to understand the full legislative framework that applies to them. It sets out rules which are specific to the UK, ensuring that GDPR works in harmony with domestic law. The DPA 2018 also provides a significant amount of continuity with the former Data Protection Act 1998.

Other laws that can impact on the way we apply Data Protection Legislation

The **Digital Economy Act 2017** aims to enable better public services using digital technologies and gives public authorities powers to share information for the public's benefit. It also gives the Information Commissioner's Office (ICO) the power to charge a fee to Data Controllers.

The Freedom of Information Act 2000 provides public access to information held by public authorities like us, however, it is essential that the requirements of the Data Protection Legislation are taken into account prior to the release of any information. In particular, we must not release information that could compromise the personal data of individuals, whether that data belongs to our own staff or to individuals outside of AF&RS.

The Privacy and Electronic Communications Regulations (PECR) give people specific privacy rights in relation to electronic communications and provides guidance for organisations that wish to send electronic marketing messages (by phone, fax, email or text), use website cookies, or provide electronic communication services to the public.

Personal data - GDPR defines '*personal data'* as:

> *"personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person 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 or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"*

Natural person – Refers to data relating to a 'living individual' who can be identified from it.

Special categories of personal data - In addition to personal data, we sometimes deal with special categories of personal data (previously known as sensitive personal data) which are afforded a higher level of protection under the Data Protection Legislation.

The following are recognised as special category data under the Data Protection legislation, however, not all of them apply to AF&RS*:

- racial or ethnic origin
- political opinions*
- religious or philosophical beliefs
- trade union membership
- genetics*
- biometric data (where used for ID purposes)*
- data concerning health
- data concerning a natural person's sex life or orientation

Data Subject - The person to whom the information relates to.

Data Controller - The person, company, public authority or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor – A person, company, public authority or other body which processes personal data on behalf of the controller.

Processing – The GDPR defines data processing as:

> *…any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;*

Processing includes collecting, storing, editing, deleting, sending, sharing, reviewing or reading information regardless whether it is stored on paper, electronic files or databases, photos, voice and CCTV recordings, or recorded by any other means. It also includes verbally sharing information via phone, radio or in person.

The GDPR covers the processing of personal data in two ways:

- personal data processed wholly or partly by automated means (that is, information in electronic form); and
- personal data processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (that is, manual information in a filing system).

The above will apply regardless if it is held centrally by the organisation, within a specific department or held on behalf of the organisation in another location. It also covers information that has been manually collected and waiting to be input on a system, scanned copies of documents held electronically, information that has been collected with the intention of being part of the relevant filing system, and information that forms part of an accessible record.

There may be instances when a public authority may hold paper records that contain personal data, which do not form part of a structured filing system. Such data is often referred to as 'unstructured manual personal information'. Whilst the GDPR does not cover such records, in order to protect the data from being disclosed under Freedom of Information requests, unstructured manual personal information is recognised under the Data Protection Act 2018, however, is exempt from most of the principles relating to processing and the obligations (including restrictions on a Data Subject's rights) within the GDPR

Further information about what is personal data can be obtained from the ICO website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

5. Responsibility

Below is a summary of the key roles to ensure that AF&RS manages our responsibilities for data protection:

The Information Commissioner's Office (ICO) is the UK's independent supervisory authority. They are responsible for enforcing data protection laws, upholding information rights in the public interest, promoting openness by public bodies and data privacy for individuals. They hold a Register of Data Controllers and as such, we are required to register with them and pay an annual fee. The powers for enforcement are designed to promote compliance, and can include criminal prosecution, financial penalties, non-criminal enforcement and audit. Under the Data Protection Legislation, we must notify the ICO of high risk personal data breaches. All AF&RS staff should refer to the Security Incident Management Policy on the staff intranet for further guidance regarding data breaches.

Data Controller

For the purposes of the GDPR and the DPA, Avon Fire Authority (which is the corporate body for AF&RS), is regarded as the 'Data Controller'. We (solely or jointly with other partners) determine the purposes and means of the processing of personal data, and are responsible for demonstrating compliance with the legislation. We are registered with the ICO (registration no Z6748396).

The Senior Information Risk Officer/Owner (SIRO) will be a member of the AF&RS Service Management Board (SMB) and will hold strategic responsibility for ensuring that the Service complies with the Data Protection Legislation. The SIRO will ensure that the Chief Fire Officer (CFO) and SMB are fully aware of the status of information risk. SMB members ensure that appropriate mitigating actions are implemented across the Service.

Data Protection Officer (DPO) is a mandatory requirement for public authorities under the GDPR. The role of the DPO is to inform and advise AF&RS management and staff about their obligations to comply with the GDPR and other data protection laws; to monitor compliance, including managing internal data protection activities; to advise on Data Protection Impact Assessments (DPIAs); train staff and conduct internal audits.

The DPO is the first point of contact for the Information Commissioner and for individuals whose data is processed. This is an independent role that reports directly to SMB.

Business Planning & Assurance Officer is the Policy owner and will ensure that this Policy is fit for purpose and meets the approval of senior management. This role is the business lead for the Service's Information Security Management System (ISMS).

Data Protection Co-ordinator is responsible for the daily functioning of data protection within the Service and promoting good practices in relation to the handling of personal information. The DP Co-ordinator will process requests for information, provide general advice and direction to staff, and organise various communications to support this.

The DP Co-ordinator is responsible for maintaining the data protection pages on the AF&RS website and staff intranet, including the Service's publication scheme and privacy notices.

The DP Co-ordinator is also responsible for maintaining this Policy, that this Policy is promoted to raise staff awareness for data protection and best practice. This Policy will be accessible via the staff intranet, website or by providing copies on request.

The Procurement and Supplies Manager will have joint responsibility with the member of staff commissioning the order/contract to ensure that the tender process and terms and conditions remains compliant under the Data Protection Legislation, and within the terms of this Policy.

All Staff responsible for the contracts for the supply of goods, work and services will ensure that contractors are aware of this Policy and that they are contractually responsible for following good data protection practices. Depending on the type of data and level of risk associated, responsible staff must carry out the relevant checks, obtain sufficient guarantees, and ensure that the correct GDPR paperwork is in place.

This helps to ensure that personal data disclosed or processed by contractors or third parties is adequately protected, as per Section 11 'Contracts'.

Information Asset Owners (IAOs) are responsible for ensuring that the personal data that is held on systems, both IT and manual paper based systems, are processed in accordance with and comply with current Data Protection Legislation and AF&RS Policies. IAOs will ensure that appropriate privacy notices are in place when collecting data, that staff receive appropriate training when processing that data, that there are suitable policies and processes to support processing, that security and access controls are in place, and that data quality and retention are appropriately managed within their given area.

All AF&RS managers are responsible for ensuring that their staff, temporary or contract staff comply with this Policy, as well as ensuring the compliance of any internal procedures regarding the collection, processing and sharing of personal information. All new staff must read this Policy as part of their induction process and all staff must complete the online data protection awareness training.

Managers who are responsible for Data Sharing Agreements which involve the sharing of personal and special categories of data (sensitive data), to ensure a written agreement is in place and that such agreements comply with the Data Protection Legislation and AF&RS Policies. Depending on the type of data to be shared and the associated level of risk, managers must seek sufficient guarantees from our partners to ensure that the data is handled appropriately as per Section 11 'Contracts'. Any partner data that we have access to under a Data Sharing Agreement must be handled as if it were our own data under the provisions of this Policy.

All AF&RS staff should familiarise themselves with this Policy and their duties and responsibilities under the Data Protection Legislation. It is compulsory for all staff to complete the Service's online data protection awareness training, which is reviewed regularly.

Data protection is everyone's responsibility, AF&RS staff must take active steps to ensure that any personal data that comes into their possession is treated in accordance with this Policy and any other related policies and procedures that may apply to the fair processing and security of the data. In the event that data sharing takes place (either internally or with external partners), staff must ensure that appropriate controls are in place to protect that data. Staff responsible for dealing with queries about handling personal data, must always make sure that these are promptly and courteously dealt with.

Avon Fire Authority Elected Members should also familiarise themselves with this Policy and their duties and responsibilities under the Data Protection Legislation.

AF&RS considers that there may be grounds for disciplinary action against any member of staff or Fire Authority Member whose actions contravene the Data Protection Legislation and this Policy.

6. Principles relating to Data Protection

To remain compliant with Data Protection Legislation, AF&RS will ensure that personal data is processed in accordance with the principles set out in GDPR.

6.1 Processed fairly, lawfully and in a transparent manner

In order to ensure that personal information is collected in a 'fair and transparent' way so that an individual understands the reason why we are collecting and processing their personal information, where practical, AF&RS will provide a **'privacy notice'** (this may sometimes be referred to as a 'fair processing statement') to explain the following:

- who we are or any representative acting on our behalf
- the purpose(s) of the processing for which the data is intended
- a description of the categories of data being collected
- what lawful basis are we relying on to process their data (Section 7 of this Policy)
- who we may share it with
- how individuals can exercise their information rights (Section 8 of this Policy)
- proposed transfers of data to other countries outside of European Economic Area
- a brief description of how we will ensure the security of their data
- our contact details if they require assistance
- what to do if they are not happy with the way we handle their data or request
- if their information is subject to automated decision making that may affect them; and
- how long we intend to keep the information.

This is done by a number of methods, such as:

- discussions with the individual and our staff or a partner agency acting on our behalf
- publication and sharing of this Policy
- the 'what we do with your information leaflets' and other printed literature
- posters displayed within our premises and at events
- directing people to view full privacy notices published on our website. The page link is permanently located at the bottom right hand side of every area of the website
- providing privacy statements (or weblinks to privacy statements) on documents and forms, such as employment documents/contracts, supplier contracts and other correspondence/literature
- our registration with the ICO
- staff information on our staff intranet

- general data protection guidance on our website

If providing privacy notices to each individual is not practical, for example when attending an emergency incident or it involves disproportionate effort or if the recording or disclosure of data is expressly laid down by law, AF&RS will issue a generic privacy notice on our website.

6.2 Collected for specified, explicit and legitimate purposes

We will ensure that we record our reasons for processing in a 'Record of Processing Activity' (ROPA) and advise Data Subjects of these purposes via a Privacy Notice.

We will not share or process data for a different purpose except for historical, statistical or scientific purposes and when data is anonymised.

6.3 Adequate, relevant and limited to what we need

We will use national guidance and relevant legislation to determine what information we need to collect. We will not ask irrelevant or unnecessary questions of the Data Subject.

6.4 Accurate and kept up to date

We will ensure the quality of information used by taking reasonable steps to ensure the accuracy of that data when it is being collected and making sure there are processes in place to regularly check, update or securely discard any personal data when it is no longer required. We will ensure that inaccurate or incomplete data is erased or rectified without delay, whether identified by a Data Subject or a member of staff.

6.5 Kept for no longer than is necessary

We will maintain a Service Retention Schedule and ROPA for all of our official/corporate records, documents and information, which is based on national guidance, best practice and legal requirements, which will cover each area of the organisation

6.6 Kept secure

AF&RS will ensure appropriate technical and organisational measures are in place to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

6.7 Accountability

These principles are legally enforceable and the GDPR requires organisations to be accountable and to demonstrate how they comply with the legislation. We will do this by keeping records of processing activity (ROPA) concerning personal data, documenting the decisions that AF&RS take about new data processing activities by carrying out Data Protection Impact Assessments (DPIAs) and ensuring policies and guidance documents are in place. We must make these available to the ICO on request.

7. The lawfulness of processing personal data

We collect and hold personal information, in order to provide public services associated with that of a Fire & Rescue Service and as an employer, such as to:

- provide fire and emergency services under the Fire and Rescue Services Act 2004.
- To enforce fire safety under the Regulatory Reform (Fire Safety) Order 2005 (RRFSO).
- provide community safety, to promote social wellbeing and other initiatives that may benefit our own staff, members of the community and reduce risk
- obtain opinions about our services
- record and evaluate our work
- build up a picture of how we are performing and what services the people in our Service area need
- make sure we meet our statutory obligations and undertake those functions efficiently and effectively
- make contact with people who submit requests for information, make enquiries, complaints and compliments
- manage and protect our assets and resources
- manage our staff under employment law and other legislation
- look after our staff and comply with our duties under the Health and Safety at Work etc. Act 1974 and other health and safety legislation

How and why AF&RS collect, process and hold personal information varies depending on which service an individual uses. This is explained in more detail in the various privacy notices made available to staff and the public.

7.1 Processing of personal data

The GDPR provides certain criteria (or processing conditions) for making the processing of personal data legitimate (lawful).

Identifying which of the following criteria will apply to the processing will assist AF&RS to deal with any data protection requests an individual can make under their information rights.

It is AF&RS's responsibility as Data Controller to ensure that one of these criteria is met before any processing takes place:

(a) the Data Subject has provided their consent.

(b) processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract (such as a contract of employment).

(c) processing is necessary for compliance with a legal obligation to which AF&RS is subject (such as employment law or health & safety law).

(d) processing is necessary in order to protect the vital interests of the Data Subject.

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in AF&RS or in a third party to whom the data are disclosed (such as carrying out our duties to deliver a fire and rescue service under the Fire and Rescue Services Act 2004).

(f) Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller. UK public sector organisations can only rely on legitimate interest when carrying out non-public tasks, such as general administration and functioning of an organisation.

7.2 Processing of Special Categories of data

By law, special categories of data (sensitive personal data) are afforded greater protection. Details of such data are provided above within the 'Definitions' in Section 4 of this document. AF&RS will ensure that any processing is met by one of the GDPR's general processing conditions from the above list (Section 7.1) and a further one below. The following are conditions which would typically relate to AF&RS:

(a) the Data Subject has given his/her explicit consent to the processing of the data.

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of AF&RS under employment, social security or social protection law.

(c) processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his consent.

(e) the processing relates to data which are manifestly made public by the Data Subject.

(f) processing is necessary for the establishment, exercise or defence of legal claims.

(g) processing is necessary for reasons of substantial public interest. Please see conditions when this can be used in Section 7.3.2 below.

(h) processing is necessary for the purposes of preventative or occupational medicine, for the assessment of working capacity of the employee, medical diagnosis or the provision of treatment.

Please note that the above is not a full list, advice can be sought from the Data Protection Team or a full list can be obtained from the ICO website

7.3 Conditions for processing special categories of data when reliant on Schedule 1 of the Data Protection Act 2018

AF&RS may process special categories of personal data (sensitive personal data) relying on the conditions in Schedule 1 of the Data Protection Act 2018 (DPA).

The DPA states that an organisation must have an **'Appropriate Policy Document'** in place to justify the processing when reliant on these conditions. It must explain how we comply with the principles of the GDPR and state our policies regarding retention and erasure. This Policy serves as our **'Appropriate Policy Document'**, in particular, the information within this this Section (below), Section 6 (Principles relating to Data Protection) and Section 9.5 (Records Management and Retention).

The below sets out the circumstances in which we may rely on the conditions within the DPA Schedule 1.

7.3.1 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.
- Processing data relating to criminal convictions under Article 10 of the 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 services for employees in the assessment of the working capacity of an employee and the provision of reasonable adjustments and treatment.

7.3.2 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 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.
- Ensuring equal and fair treatment in recruitment and employment practices.

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 grievance and disciplinary investigations and meetings relating to our staff.

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 targeted fire prevention visits such as the Firesetters Scheme and Home Fire Safety Visits.
- Identifying individuals at risk while attending emergency incidents.

- Obtaining further support for children, vulnerable adults and individuals at risk by sharing information with relevant agencies to protect them from harm. We will, however, always seek consent from the individual to carry out the intervention unless seeking consent to participate would not be reasonably expected or would put our staff at risk or the individual at risk of further harm.

Safeguarding of economic well-being of certain individuals

- Carrying out targeted fire prevention visits such as the Firesetters Scheme and Home Fire Safety 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.

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

Extension of conditions in Part 2 of Schedule 1 referring to substantial public interest.

- Processing 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.

Further information about the principles and criteria for processing of personal and special categories of data under the GDPR can be found in the 'Guide to Data Protection' on the ICO website.

7.4 Consent

If consent is the lawful basis being used, it must be specific, clear, properly documented, and easily withdrawn. It must be freely given and an informed, unambiguous and a definite indication of the individual's wishes. This means that there must be clear affirmative action, such as a positive ‘opt in’ and for this reason, it is important to document consent (including documenting verbal consent).

Pre-ticked boxes and ‘opt out’ consent are not acceptable. When we are relying on consent for processing special categories of data, this must be explicitly given, such as written consent.

If consent is the lawful basis being used, it is likely that the individual has the right to withdraw that consent, this must be considered when setting up systems and ways of working to ensure that, if the individual choses to withdraw consent, their information can be found and removed easily. See Section 8 below for more information about individual rights.

7.5 Children and youth services

We will use our public task obligation when collecting personal information relating to a child under the age of 18 years and we will ensure that an appropriate adult, such as a parent or guardian is aware when we collect any children’s information, unless doing so will place the child at risk.

Privacy information about children’s data must be written in clear language which can be understood by the intended age group.

8. Individual's rights regarding their personal information

GDPR has strengthened the rights that individuals have in relation to their personal data. The Data Subject may request for any of the following rights to be invoked, however, there are circumstances in which AF&RS would not have to action the request, depending on the reason for processing it (as set out in Section 7 above).

8.1 Summary table showing when the rights apply

The table below gives a very general view of when the individual may or may not be able to use their information rights, depending on AF&RS reason for processing their data. **It should be noted that these rights are not absolute, there are exceptions to all the rights and each request will be reviewed on a case by case basis.**

The individual's right	Lawful basis for processing (AFRS's reason for processing the personal data)						
		Consent	**Contract**	**Legal Obligation**	**Vital Interests**	**Public Task**	**Legitimate interests**
	Right to be informed	✓	✓	✓	✓	✓	✓
	Right to access	✓	✓	✓	✓	✓	✓
	Right to correction	✓	✓	✓	✓	✓	✓
	Right to erasure	✓	✓	✗	✓	✗	✓
	Right to restrict	✓	✓	✓	✓	✓	✓
	Right to portability	✓	✓	✗	✗	✗	✗
	Right to object	✗	✗	✗	✗	✓	✓
	Right to not be subject to automated decisions	✗	✗	✗	✓	✓	✓

8.2 The right to be informed

When collecting an individual's personal data, we will explain exactly what will happen to it using a Privacy Notice (see Section 6.1 of this Policy).

8.3 The right of access

Individuals have the right to get confirmation that their data is being processed and have access to their personal data (often referred to as a Subject Access Request). Individuals can specify the format they wish to receive the data in (subject to the original format the information is held).

An individual is only entitled to information held about them and not personal information relating to other people unless they are acting on their behalf and there are exemptions regarding the information that can be released.

The request must give a specific description of the information required, to enable us to locate it.

8.4 The right to rectification

Individuals can ask to correct information that they believe is inaccurate or incomplete.

They must be clear about exactly what they believe is inaccurate and how we must correct it, providing evidence of the inaccuracies where available. We will confirm that we have corrected the personal data or if we consider that the data does not need to be corrected, we will explain why.

8.5 The right to data erasure

This is also known as 'the right to be forgotten'. Individuals can request that we delete their personal data where there is no compelling reason for us to keep it.

The right is not absolute and we will not delete personal data which we still need to fulfil our official responsibilities as a Fire Service or as an employer. We will notify the requester if this is the case.

8.6 The right to restrict processing

In some circumstances, individuals have a right to 'block' processing of their personal data until any errors have been rectified when requesting the right to rectification.

If an individual is concerned that we may be processing data about them in a manner that is not fair and lawful, they can request that processing is restricted while they pursue a complaint / determine our condition for processing.

If the individual is not entitled to data erasure of the content, the individual may be entitled to restrict, 'block' or suppress processing of personal data. When processing is restricted, organisations are only permitted to store the personal data, they may only continue using it under certain circumstances.

8.7 The right to data portability

Individuals can obtain their personal data in a portable, usable format allowing them to move, copy or transfer it easily and securely from one IT environment to another (e.g. when changing utility providers). The right to data portability is very unlikely to apply in the context of the Fire Service.

8.8 The right to object

Individuals have the right to object to:

- their data being processed in any way other than the original purpose.
- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority
- direct marketing
- processing for purposes of scientific/historical research and statistics

If they raise an objection we will stop using the personal data, unless we are able to prove overriding legitimate grounds for doing so.

8.9 The right to not be subject to automated decision making and profiling

Individuals have the right not to be subject to a decision based solely on profiling or automated processing of data, without human intervention, which significantly affects them. Examples such as evaluating their performance at work, economic situation, health, personal preferences, behaviour, location or movements. The decision must have a serious negative impact on an individual for this provision to apply.

While we do use data to help us target people in need, we do not carry out decisions without human intervention. AF&RS will inform an individual prior to processing if their personal data is subject to any automated decision making or profiling.

8.10 Submitting a request

All of the above requests must be submitted to AF&RS in writing (email, web form, social media or letter).

We do not routinely charge a fee for any of these types of request, however, the legislation allows some discretion when dealing with requests for manifestly unfounded or excessive requests, in particular if they are repetitive. AF&RS can charge a reasonable fee, taking into account the administrative costs of providing the information; or refuse to respond. If the latter is the case, we will explain the reasons and assist the individual to re-submit their request in a more manageable form.

The member of staff processing the request must be confident of the identity of the person making the request, particularly, if the request has come from a member of the public. Proof of identity may be required.

There is a requirement to provide information or a response, within one calendar month or up to 3 months for complex requests. Due to this timeframes, it is very important to ensure that the request is passed to the Data Protection Team without delay should a request be received by another department.

Refer to our Data Protection pages of our website for further information and guidance or submit a request online.

Information about companies or public authorities is not personal data and any requests for information should be submitted under the Freedom of Information Act. However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

8.11 Information about a deceased person

The Data Protection Legislation relates to the handling of personal data in relation to a 'natural person' being a 'living individual' and does not cover individuals who are deceased. However, AF&RS still have a duty of confidence to the deceased and their family. Each request concerning the personal information about the deceased will be considered on an individual basis.

9. Accountability and Governance

The GDPR includes provisions that promote accountability and governance. AF&RS has a general obligation to implement technical, physical and organisational security measures to safeguard personal information from point of collection to disposal. We must be able to demonstrate that these measures are in place and that we have integrated data protection into our processing activities.

9.1 Documentation

AF&RS regularly review all policies, procedures, forms and Data Sharing Agreements which include the handling of personal data, to ensure they comply with the Data Protection Legislation as well as other relevant legislation.

We ensure that we have adequate policies and processes in place to ensure that the rights of Data Subjects can be fully exercised under the GDPR (as per Section 8 'Individual's rights regarding their personal information' of this Policy).

We ensure we have assurance from suppliers and contractors regarding their compliance with the GDPR, that Data Controller / Data Processor responsibilities are documented and appropriate contracts or agreements are in place (as per Section 11 'Contracts').

9.2 Staff Training

AF&RS ensure that mandatory data protection training is undertaken by all staff as part of their induction (temporary and permanent) and refreshed every two years.

9.3 Personal Data Breach Notification

AF&RS have a Security Breach process in place to ensure that any breaches that pose a high risk to the rights and freedoms of individuals are reported to the ICO within the mandatory 72 hours. All data security breaches are logged, investigated and measures will be put in place to prevent a re-occurrence as per the AF&RS Security Incident Management Policy.

9.4 Data Protection Impact Assessments (DPIAs)

It is a mandatory requirement under the GDPR for organisations to perform a DPIA where processing is '*likely to result in a high risk to the rights and freedoms of natural persons'*. In order to uphold good data protection practices, AF&RS will embed DPIAs into normal business activities and carry out a DPIA when introducing any new process, initiative, policy, procurement or project and for major reviews of existing policies/processes that can impact in some way on personal data, data protection rights or their privacy.

The DPIA is a risk assessment tool to help organisations which process personal data to properly consider and address data protection and privacy risks. The DPIA process allows AF&RS to consider whether the impact on data protection and privacy is proportionate to the outcomes of what the project/process/policy hopes to achieve. Screening questions within the template can assist in determining whether a full assessment is needed.

A DPIA can reduce the risk of harm to individuals through the misuse of their personal information. It can also assist AF&RS to design more efficient and effective processes for handling personal data.

DPIAs will be reviewed by the Data Protection Team and logged. They will be signed off by the Business Planning and Assurance Officer if low risk and by the SIRO if high risk. The DPO will audit DPIAs on a regular basis and provide advice when required.

Further guidance for staff, is available on the Data Protection pages of our staff intranet.

9.5 Records Management and Retention

AF&RS operates a Service Retention Schedule and guidance to ensure that personal data is not kept for longer than required and is suitably disposed. Retention periods will take into account any legislative requirements or industry best practice.

Department Managers or Asset Information Owners are responsible for ensuring that the personal data in their area adheres to the Service's Retention Schedule. Retaining data that exceeds its required period may increase the risk of that data being out of date, inadvertently impact on decisions that the Service may make about the individual, and impact on the processing of requests regarding an individual's rights, such as the right of access.

9.6 Record of Processing Activities (ROPA)

AF&RS will keep a 'Record of Processing Activities' listing all personal data (internal and external) handled within the Service, which will document the purposes and lawful conditions of processing personal data.

9.7 Privacy by Design

AF&RS will consider privacy, data protection and information security at the beginning of any new project, policy, process or system by completing a DPIA.

This will also be reflected in any new forms, online forms, guides and other documents that we use, giving consideration to data minimisation.

9.8 Compensation and Liability

An individual has the right to apply for compensation if they have suffered damage as a result of any unlawful processing operation by AF&RS or any act performed by AF&RS that is incompatible with the Data Protection Legislation. Data Controllers and Data Processers are both liable for infringements, unless they can prove that they are not responsible for the event giving rise to the damage.

10. Sharing of Personal Data

AF&RS will ensure that disclosures of personal information will be in accordance with the provisions of the Data Protection Legislation. We will not disclose personal information unless we are satisfied that equal or stronger measures are in place to protect the information from unauthorised access. AF&RS has a duty to disclose certain data to public authorities under legislation, such as for crime and taxation purposes.

In order to provide an emergency service, perform our functions as a statutory organisation and to meet our obligations as an employer, there are circumstances where we are permitted to share personal information. AF&RS will ensure that it meets its requirements under the legislation and there are legitimate grounds for processing, regardless of whether the sharing is with the individual themselves, law enforcement bodies, councils and other organisations.

Some shared information will be anonymised to protect the privacy of the individual. Where personal data needs to be shared, AF&RS will make individuals aware if their information is intended to be shared and provide the opportunity for them to say 'no', except when we are required by law to pass on the information, such as to crime and disorder partners, central and local government, bodies employed to process data on our behalf and auditors.

Where it is not possible or practical to obtain consent to share sensitive personal information, we will only share the information we consider essential to protect an individual's interests. Such as:

- Information provided to crime agencies relating to prevention and detection of crime
- Information which is in the interests of a person's health and wellbeing including when necessary to prevent serious risk to individuals and for safeguarding purposes

Sharing information with our partners will only take place under strict data sharing protocols with tight security for the transfer of information. AF&RS will not sell or rent any part of the personal information they collect to third parties. Access to all personal information will also be restricted to authorised individuals on a 'need to know' basis.

10.1 Data Sharing Agreements

Data Sharing Agreements with our partners are typically for preventative work such as safeguarding, promoting welfare and wider public protection.

Data Sharing Agreements with our partners should take into consideration the same checks and security measures to protect that data, as we do for contractors (see Section 11 below).

The Agreement should clearly define the purpose for sharing, data types and Data Subject categories, lawful basis for processing, data exchange and storage, each of the parties' responsibilities for the data, and the role each party will play, such as Data Controller, as well as the general terms of the Agreement.

There are a number of different relationships which we may have with contractors and partners. There may be circumstances where we are classed as 'Joint Data Controllers', 'Controller to Controller' or 'Data Controllers in Common'. It is important to understand the responsibilities for each party to ensure it is documented correctly. Advice can be sought from the Data Protection Team if required.

11. Contracts

This section covers all contractors, suppliers, consultants, partners or other servants or agents (third parties) of Avon Fire Authority (AFA).

AF&RS staff that are responsible for contracts, tenders and Data Sharing Agreements must make all parties aware of this Policy (and in some circumstances our Information Security Policy) and provide a copy of (or access to) this Policy.

The Data Protection Legislation requires us as a Data Controller, to ensure that all organisations/individuals that **process personal data** on our behalf (Data Processors) are fully aware of their legal responsibilities and are processing in line with the law and our requirements.

For this reason we will ask all contractors to complete our GDPR Contract Assurance Form, which will cover areas such as only acting as per our instructions; that they have suitable technical and organisations measures in place to protect our data; to only use sub-processors with our consent; and security breach notification. We will also provide the contractor with a Schedule of Processing if they are a Data Processor, which will cover categories of data, types of Data Subjects, processing activities and data retention; together with a Data Processor Agreement, which must be adhered to.

The Data Processor Agreement will cover specific instructions of how the data should be handled, responsibilities of each party and any other terms of processing not already covered by the Schedule of Processing.

A copy of the above forms, along with a copy of our Standard Terms and Conditions and further guidance, is available on our website:
https://www.avonfire.gov.uk/information-for-suppliers/new-data-protection-legislation-and-contracts

The AF&RS members of staff that are responsible for contracts or one off services that cover an external party processing personal data on our behalf, should liaise with the Procurement and Supplies Department to ensure that the correct paperwork is in place before the contract and processing commences. The requirement to complete the necessary paperwork will be initiated as part of the setting up of a new supplier process.

For any services that impact on the processing of personal data, there must be a written contract in place. Any breach of the Data Protection Legislation concerning that processing, will be deemed a breach of contract.

Depending on the type, sensitivity, volume and level of risk associated with the processing or sharing of data, it is recommended that staff seek guidance from the Data Protection Team, who may recommend that a DPIA is completed to identify any risks and put in place adequate controls to mitigate or reduce those risks.

11.1 Contract due diligence for tender process

Depending on the nature of the data and the processing/disclosure involved, the below points should be considered within the tender process for any contract that covers the processing of personal data.

The tender applicant to provide:

- sufficient guarantees/warranties in respect of technical and organisational security measures governing the processing of our data, such as copies of their relevant policies, proof of accreditations (ISO 27001) and Cyber Essentials/Plus Certificate.
- sufficient guarantees/warranties in respect staff quality and training in relation to Data Protection
- staff competencies, qualifications and training in relation to subject matter
- details of any data processing that will be subject to being transferred outside of European Economic Area (EEA) and if so, what measures are in place
- details of any data processing subject to sub-processing or disclosure to a third party not covered by the contract
- Known security breaches or if they have been subject to ICO complaints within the last 3 years
- confirmation that they able to comply with our Data Processer GDPR Statement of Assurance and the Data Protection Legislation.

12. Data Transfers

The Data Protection Legislation imposes restrictions on the transfer of personal data to countries outside the European Economic Area (EEA), or to international organisations, to ensure that the level of protection to individuals provided by that legislation is not undermined.

All AF&RS personal information is held on servers within the UK and may be accessed by our staff, government bodies, law enforcement agencies and suppliers or third parties we engage to process data on our behalf or who act for us for the purpose set out within the given privacy notice.

The Data Protection Legislation does provide exemptions to enable the transfer of personal data outside the EEA in certain situations. AF&RS would not generally transfer data outside of the EEA, however, if such a transfer is required, a DPIA will be undertaken to assess the risk and ensure adequate safeguards are in place to protect the data and ensure the individual's rights are not affected. Exemptions allow such transfers to take place with the individual's consent; for performance of a contract; for the establishment, exercise or defence of legal claims; for important reasons of public interest; or to protect the vital interests of the Data Subject or other persons.

13. Further information

The following is available on our website:

AF&RS Privacy Statement on the website
AF&RS Information Security Policy and other related policies
Data Protection pages on our website, which includes guidance of how to make a request for personal information (Subject Access Request).

What we do with your information leaflet

Useful external websites:

- Information Commissioner's Office website
- The Data Protection Act 2018

13.1 Complaints

If for whatever reason an individual is unhappy with the way their request for information has been handled, they can request an internal review within 40 working days of us issuing the original response, by writing to the **Data Protection Officer, Avon Fire & Rescue Service, Police & Fire Headquarters, PO Box 37, Valley Road, Portishead, Bristol, BS20 8JJ, telephone 0117 9262061, or by emailing FOI-DP@avonfire.gov.uk**.

If the individual remains dissatisfied with the handling of their request or complaint, they have the right of appeal to the Information Commissioner at: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, telephone 0303 123 1113 (local rate) or 01625 545 745. Website www.ico.org.uk. There is no charge for making an appeal.

AF&RS also operates a formal complaints process if individuals are unhappy about any of our services or performance.

Document Control Information:

Policy title:	Data Protection Policy
Policy owner: (role)	Business Planning and Assurance Officer
Authoriser: (role)	Director Corporate Services
Author	Data Protection Co-ordinator / Business Planning and Assurance Officer
Issue status:	Published
Protective marking:	-
Issue date:	05/11/2018
Next review due:	05/11/2021
Audience:	For external publication
Version Number:	1

Document History:

Review Date	Version No	Summary of Changes	Equality Impact Assessed (Y/N)
10.08.2018	0.1	Draft version ready for consultation	Y
16.08.2018	0.1	Minor amendment to under Responsibility section regarding Procurement and Supplies Manager	
03.09.2018	0.1	Feedback from DPO re draft version. Minor amendments. Section 4, pg 7 regarding unstructured manual data needs to be further investigated	
18.10.2018	0.1	Correct minor typos	
26.10.2018	0.1	Approved by FBU and Unison	
31.10.2018	0.1	Approved by Director	
05.11.2018	1.0	Updated the lawful reasons for processing safeguarding and firesetters to public task	

Distribution History:

Date	Version No	Distributed to: (role/s or group/s)
15.08.2018	0.1	Procurement and Supplies team – draft version
28.08.2018	0.1	DPO – draft version
05.09.2018	0.1	Draft copy on staff intranet for consultation
01.10.2018	0.1	Copy to Dir Corporate Svcs Dir for PPM01 sign off
04.10.2018	0.1	Copy to unions for consultation
05.11.2018	1.0	Published on intranet (all staff) and website