Data Management Policy

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

Contents

1 Introduction

1.1 Policy Statement

All data held by Avon Fire & Rescue Service (AF&RS) is to be managed according to data management procedure, which will be in compliance with current data protection legislation.

1.2 Scope

This policy applies to **all AF&RS staff** (including temporary or contract) and **all procedures** that apply to the handling of any data or special category (sensitive) data, regardless of how that data is collected, recorded, used, and stored.

2 Policy Principles

All new members of staff must read this policy as part of their induction process.

All staff must take active steps to ensure they are handling any data according to the appropriate procedure for management of that data.

Avon Fire Authority Elected Members are strongly advised to familiarise themselves with this policy to understand the importance of following data management procedures and current data protection legislation, and the resulting duties and responsibilities that apply to the handling of data.

3 Responsibilities

Data management is everyone's responsibility.

3.1 All Staff

All staff must familiarise themselves with data management and data protection procedures if carrying out any process involving personal or special category data.

All staff must follow agreed procedures to ensure data held in an information asset is collected, stored, processed, and disposed of securely and correctly.

All staff must be mindful of their duties and responsibilities concerning data protection and data security. They must complete AF&RS data protection awareness training and any scheduled update training.

All staff must observe any data protection guidance and Service communications to maintain awareness.

There are grounds for legal and/or disciplinary action against any member of staff or any Fire Authority Member whose actions contravene current data protection legislation.

3.2 Any staff member entering AF&RS into a contract or agreement

Any staff member investigating, considering, or negotiating a contract or agreement must follow data management and data protection procedures, and be mindful of current data protection legislation and relevant guidance. This would include, but not be limited to a Procurement Contract for the supply of goods, works, or services, a Partnership Agreement, a Data Sharing or Data Processing Agreements, or a Memorandum of Understanding.

If the contract or agreement involves any processing of personal data, they must ensure appropriate agreements which comply with current data protection legislation and any relevant AF&RS policy or procedure are in place. Depending on the type of data and the associated level of risk, they must carry out relevant checks, obtain sufficient guarantees, and ensure the correct paperwork is in place to ensure data will be handled appropriately.

3.3 All managers

All managers are responsible for ensuring staff complete data protection awareness training and follow data management and data protection procedures.

3.4 Service Leadership Team (SLT) members

SLT members are responsible for ensuring any appropriate mitigating actions for identified data-related organisational risks are implemented.

3.5 Information Asset Owners (IAOs)

IAOs are responsible for the management, data quality, and security of an information asset they control or hold responsibility for.

They must understand what data is held within that information asset, how it is added, moved, or removed, who has access to it, the associated risks, and how those risks are mitigated.

They will establish and maintain agreed procedures to guide staff in the correct use of the data in the information asset (including least privilege controls and privacy notices).

3.6 Information Governance Team (IGT)

The IGT are responsible for processing requests for information, promoting good practices in relation to the handling of personal information, and providing AF&RS staff with general advice on data management and data protection issues.

The IGT will advise IAOs on establishing and maintaining agreed system procedures to ensure compliance with data management procedures and current data protection legislation.

The IGT will maintain data protection and transparency pages on the AF&RS website and staff intranet (including the publication scheme and privacy notices).

3.7 Data Protection Officer (DPO)

The DPO is responsible for establishing and maintaining overarching data protection procedures within the Service.

The DPO will inform and advise staff on obligations necessary to comply with current data protection legislation and will monitor compliance (including managing data protection activities and conducting internal audits).

The DPO will oversee and provide advice on data protection awareness training and Data Protection Impact Assessments (DPIAs).

The DPO is the first point of contact for the Information Commissioner's Office, which is the UK's independent supervisory authority, and for individuals complaining about AF&RS's handling of their personal data.

3.8 Senior Information Risk Officer (SIRO)

The SIRO holds strategic responsibility for overall information risk management, information incident management, and risk assessment processes.

The SIRO will advise the Chief Fire Officer and all SLT members on information risk and controls, and the risk of failing to meet data security obligations or undertaking appropriate mitigating actions.

Document Control Information:

Policy Title:	Data Management Policy		
Policy Owner:	Lucy Jefferies		
Policy Owner [Role]:	Information Governance Manager		
Issue Date:	21/02/2024		
Next Review Due:	21/02/2027		
Audience:	For external publication		
Version Number:	2.0		
Impact Assessment No.	194	**Date of IA:**	15/05/2023

Document Approval Information:

To be completed by the relevant representative from Service Leadership Board (SLB) to authorise publication.

Name:	Jane Williams-Lock
Role:	Deputy Director of Corporate Services
Date of Authorisation:	21/02/2024