

# Information Governance Statement



West Yorkshire Fire and Rescue Authority, as a provider of public services, recognises the importance of Information Governance and states its commitment to information security and governance. Information Governance is a framework to bring together all of the requirements, standards and best practice that apply to the handling of information. It allows organisations and individuals to ensure that information is accurate, dealt with legally, securely, efficiently and in order to deliver the best possible service.

The Information Governance Strategy and Policy and the resulting framework for the Authority is based upon national best practice models including the NHS Data Security and Protection Toolkit, HMG Security Framework and the ISO/IEC 27001 Information Security Management Standard. The West Yorkshire Information Management Forum, of which West Yorkshire Fire and Rescue Authority is a member, has carried out a local development project for adopting a consistent framework across the public authorities of West Yorkshire.

Information is a vital asset, in terms of both the management of individual customers and the efficient management of services and resources. It plays a key part in corporate governance, service planning and performance management. It is, therefore, of paramount importance that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

West Yorkshire Fire and Rescue Authority aims to work collaboratively with partner agencies to ensure any information governance issues which span more than one organisation are handled effectively and appropriately.

The Authority stores and processes critical and sensitive information. This information is valuable and the Authority is committed to ensuring its confidentiality, integrity and availability as defined by ISO27001. The Authority will manage risks to its information and ensure it is adequately protected against threats, non-technical as well as technical, which can affect it. The Authority must comply with relevant legislation that affects information security and governance, including, but not confined to, the Data Protection, Freedom of Information and Human Rights Acts. It also aims to comply fully with the requirements of the General Data Protection Regulation (GDPR) which came into force from May 2018.

Compromised information can cause enormous damage to the Authority's operations and reputation. Information not appropriately and adequately protected can lead to serious compliance and legal failures. It is a valuable asset to the Authority and is the basis upon which strategic and critical decisions are made and operational tasks are performed. Accordingly, it is essential that the information be accurate and complete, properly managed, controlled and secure.

For these reasons, the Authority has approved the Information Governance Strategy and Policy and the formation of the Information Governance and Security Group supported by the Corporate Information Management Group. The Information Governance and Security Group has authority for all information governance and security matters and will manage these through a robust set of policies, standards, procedures, best practices, controls, risk management and other measures, and will ensure compliance with them.

The policy applies equally to anyone who has access to the Authority's information and information processing systems. The Information Governance and Security Group, on behalf of the Authority, will ensure that everyone has access to the policy. Anyone with access to our information and information processing systems is responsible for understanding it and complying with it.

Signed:  
Date: 24 March 2020

A handwritten signature in blue ink, appearing to read 'John Roberts', written over a horizontal line.

John Roberts  
Chief Executive/Chief Fire Officer

Issue Date: March 2020

Review Date: March 2023

Ref: Version 5.0