West Yorkshire
Fire & Rescue Service

Information Governance Strategy and Policy

OFFICIAL
Ownership: Information Governance Group
Date Issued: 15/01/2015
Version: 2.0 Status: Final

Making West Yorkshire Safer
www.westyorksfire.gov.uk

Revision and Signoff Sheet

Change Record

Date	Author	Version	Comments
19/01/2015	Allan Darby	1.13	Major changes to align to the new local authority IG Toolkit

Reviewers

Name	Version Approved	Organisation	Date
Information Governance Group	2.0	WYFRS	19/01/2015

Distribution

Name	Position	Organisation

Document Properties

Item	Details
Document Title	Information Governance Strategy and Policy
Author	Administrator
Creation Date	19 January 2015
Last Updated	19 January 2015

Contents

1 Introduction

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 Policy and the resulting framework for West Yorkshire Fire and Rescue Authority is based upon national best practice model the NHS Information Governance Toolkit. 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.

2 Policy

The Authority recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Authority fully supports the principles of corporate information governance and recognises its public accountability.

2.1 Principles

The Authority believes that accurate, timely and relevant information is essential to deliver the highest quality service. As such it is the responsibility of all Principal Officers and managers to ensure and promote the quality of information and to actively use information in decision-making processes.

The importance of confidentiality, security, and data quality play a role in the safeguarding of information within West Yorkshire Fire and Rescue Authority. This includes customer and staff information as well as commercially sensitive information.

West Yorkshire Fire and Rescue Authority has agreements to share some customer information with other public authorities and other agencies in a controlled manner, which ensure the protection of customers' and public interests.

The Authority aspires to reach the highest standards included within the Authority Information Governance Framework and is committed to using the toolkit, and self-assessing against it, to achieve this.

There are a number of key interlinked strands to the Information Governance Policy:

- Information Governance Management
- Information Security Assurance
- Confidentiality and Data Protection Assurance
- Records Management Assurance

3 Responsibilities

3.1 The Authority

Overall responsibility for the efficient administration of the Information Governance lies with the Authority.

3.2 Principal Officers and Heads of Department

Day to day responsibility for administration and compliance with the Act is delegated from the Authority through the Chief Legal and Governance Officer to the respective Principal Officer or Head of Department for their service area. Within each Department, an Information Champion will be appointed to co-ordinate information governance and to assist in compliance with the requirements of the legislation on behalf of the Chief Legal and Governance Officer or Head of Department.

3.3 Information Governance Group

The Information Governance Group, made up of individuals that are suitably senior and/or with necessary expertise, will be delegated with the responsibility for the implementation and monitoring of information governance across the Authority. The work undertaken will be in line with the Group's Terms of Reference as detailed at Appendix 1. The Group will report to the Management Team.

3.4 Information Champions

The Information Champions are responsible to their Head of Department or Principal Officer for:

- Liaison with the Information Governance Group on all matters concerning administration of this Strategy/Policy.
- To work with the Principal Officer or Head of Department to ensure compliance in respect to systems within their Area of Responsibility.
- To work with the Principal Officer or Head of Department to ensure awareness of the need for information governance within the Authority, and to ensure that the control and handling of information within the Department or Station does not contravene any appropriate legislation or Authority procedures.

3.5 Managers

Managers are responsible for ensuring that staff under their direction and control are aware of the policies, procedures and guidance laid down by the Chief Legal and Governance Officer through the Information Governance Group and for checking that those staff understand and appropriately apply policies, procedures and guidance in respect of information governance in carrying out their day to day work.

3.6 All Staff

It is the responsibility of all staff to process information in accordance with the Data Protection Act 1998 and to adhere to the policies, procedures and guidance that are laid down by the Authority for information governance and security.

4 Information Governance Management

The development and implementation of an appropriate information governance infrastructure to be delivered across the Authority is fundamental to the successful implementation of the framework. It is necessary to provide ownership and advocacy at corporate, managerial and operational levels throughout the Authority.

4.1 Information Governance Management Objectives

- There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda.
- There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans.
- Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations.
- Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation.
- Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained.

5 Information Security Assurance

The introduction of an Information Security Management System (ISMS) that is based on ISO 27001 standards will ensure that the Authority will protect the confidentiality, integrity and availability of information within the organisation and when sharing with partners. Compliance with ISO 27001 will ensure compliance with the information governance requirements.

5.1 Information Security Assurance Objectives

- The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs.
- A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed.
- There are documented information security incident / event reporting and management procedures that are accessible to all staff.

- Operating and application information systems (under the organisation's control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems.

- All transfers of hardcopy and digital person identifiable and sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers.

- Business continuity plans are up to date and tested for all critical information assets (data processing facilities, communications services and data) and service - specific measures are in place.

- Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error.

- Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code.

- Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely.

- Policy and procedures ensure that mobile computing and teleworking are secure.

- There is an information asset register that includes all key information, software, hardware and services.

- All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures.

- The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate.

6 Confidentiality and Data Protection

There is a legal framework which governs information products and the Authority must be compliant with it. The Authority handles and processes large volumes of confidential and sensitive information about individuals and must deal with this lawfully and ethically. Failure to comply could endanger individuals and can also increase risk, the chances of litigation and the loss of reputation.

6.1 Confidentiality and Data Protection Assurance Objectives

- The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs.

- Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users.

- Personal information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected.

- Individuals are informed about their proposed uses of their personal information.

- Where required, protocols governing the routine sharing of personal information have been agreed with other organisations.

- All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements.

7 Records Management Assurance

Records Management covers the process of creating, describing, using, storing, archiving and disposing of organisational records according to a defined set of standards (usually ISO 15489). Compliance with this fundamental component of the Information Governance framework will ensure that the Authority adheres to statutory information access requirements.

7.1 Records Management Assurance Objectives

- The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience.

- Documented and implemented procedures are in place for the effective management of corporate records.

- Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000.

- As part of the information lifecycle management strategy, an audit of corporate records has been undertaken.

8 Assessments, Work Plans and Implementation Arrangements

8.1 Assessment

The Information Governance Group is responsible for ensuring an assessment of compliance as detailed in the Information Governance Toolkit is undertaken each year. Annual work / development plans are produced and these are considered by the Information Governance Group at intervals throughout the year.

The Information Governance Toolkit requirements are grouped into the following initiatives:

- Information Governance Management
- Information Security Assurance
- Confidentiality and Data Protection Assurance
- Records Management Assurance

Lead Officers for each of the above areas have been identified.

8.2 Adherence

It is the responsibility of the Information Governance Group to ensure the Authority adheres to its Information Governance Policy. For Information Security matters, the Authority will seek advice and support from the Information Governance Group with input from the IT Department.

8.3 Terms of Reference

The terms of reference of the Information Governance Group are attached as Appendix 1.

8.4 Accountability

The Information Governance Group reports to and is accountable to the Authority's Management Team.

8.5 Review

This Policy will initially be reviewed annually.

9 Related Policies and Supporting Procedures

Other Authority policies which should be read in association are:

- Freedom of Information Policy
- Records Management Policy
- Access to Information Policy
- Data Protection Policy
- Information Security Policy
- Data Quality Policy
- Information Sharing Protocol

Appendix 1 - INFORMATION GOVERNANCE GROUP ~ Terms of Reference

1. Purpose

The purpose of this Group is to provide advice and assurance to the Authority on all matters concerning Information Governance.

2. Definition

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 principles of Information Governance which is an Authority wide initiative provides a consistent way for employees to deal with many different information handling requirements.

3. Objectives

3.1 To ensure that the Authority has effective policies and management arrangements covering all aspects of Information Governance in line with the Authority's overarching Information Governance Policy, i.e.

- Information Governance Management
- Information Security Assurance
- Confidentiality and Data Protection Assurance
- Records Management Assurance

3.2 To ensure compliance with information governance requirements placed on the Authority, particularly by the Information Governance Framework; to develop action plans where compliance is less than 100% and monitor their implementation.

3.3 To ensure that the Authority undertakes or commissions annual assessments and audits of its Information Governance policies and arrangements.

3.4 To establish annual Information Governance Framework Improvement Plans, secure the necessary implementation resources, and monitor the implementation of those plans.

3.5 To receive and consider reports into breaches of confidentiality and security and where appropriate undertake or recommend remedial action.

3.6 To ensure all relevant risks are recorded on the Authority's Risk Register.

3.7 To liaise with other Authority committees, working groups and programme boards in order to promote Information Governance issues.

3.8 To ensure full and effective liaison with all external organisations such as the Information Commissioner, local authorities and other relevant organisations.

3.9 To formulate and receive guidance from such supporting committees or groups as appropriate.

3.10 To report to the Management Team on Information Governance issues and to carry out such other tasks as may be required of it by the Authority.

3.11 To identify where new Policies and Procedures are required or are in process of implementation and to assign responsibility for overseeing implementation of each Policy and Procedure.

4. Accountability

The group reports to Management Team.

5. Membership

The group membership will consist of Area Managers/Heads of Department, Corporate Services Manager, Corporate Human Resources Manager, Data Team Manager, Information Management Officer, System Support/Information Security Manager and union representation.

6. Meetings and Reporting

The Group will meet quarterly. Minutes of each meeting will be circulated within two weeks of the meeting.

7. Approval and Review

These terms of reference will be reviewed annually and any changes agreed with the Management Team.