West Yorkshire
Fire & Rescue Service

Data Protection Policy

OFFICIAL
Ownership: Corporate Services
Date Issued: 25/05/2018
Version: 4.0 Status: Final

Making West Yorkshire Safer
www.westyorksfire.gov.uk

Revision and Signoff Sheet

Change Record

Date	Author	Version	Comments
02/12/2014	Allan Darby	3.0	Minor amendments throughout and transfer onto new policy template.
25/05/2018	Tayber Amber	4.0	Changes to incorporate Data Protection Act 2018 (incorporating GDPR)

Reviewers

Name	Version Approved	Position	Organisation	Date
Allan Darby	3.0	Information Management Officer	WYFRS	02/12/2014
Information Governance and Security Group	4.0		WYFRS	18/04/2018

Distribution

Name	Position	Organisation

Document Properties

Item	Details
Document Title	Data Protection Policy
Author	Administrator
Creation Date	02 December 2014
Last Updated	18 April 2018

Contents

1 Commitment

West Yorkshire Fire and Rescue Authority is committed to ensuring that the personal and sensitive information (data) it holds about individuals is accurate, up to date, used only for the purpose intended and securely protected from inappropriate access. The Authority is further committed to ensuring that individuals can find out about their personal data, be given access to it and the right to challenge its accuracy. In terms of non-personal information, the Authority is further committed to promoting public access to the information it holds.

2 Introduction

This document sets out the Authority's policy regarding data protection. The Data Protection Act 2018 (incorporating GDPR) provides the basis of this document. The Freedom of Information Act 2000 affects the Authority's use of non-personal information and the operation of this policy. The Human Rights Act 1998 affects the protection and individual rights given under the Data Protection Regulations.

The purpose of the data protection legislation is to regulate the way that personal information about individuals, whether held on computer or in a manual filing system, is obtained, stored, used and disclosed. The legislation grants rights to individuals, to see the data stored about them and to require modification of the data if it is wrong and in certain cases, to compensation. The provisions amount to a right of privacy for the individual.

3 Definitions

To aid the understanding of this document and provisions of the Data Protection Act 2018 (incorporating GDPR) the following definitions are provided:

Data is information that is:

- Being processed by means of equipment operating automatically in response to instructions given for that purpose e.g. payroll system
- Recorded with the intention that it should be processed by means of such equipment e.g. on disk or CD ROM
- Recorded as part of a manual filing system or with the intention that it should form part of such a system e.g. any departmental filing system with an index
- One of a number of records to which public access is allowed

Data Controller means West Yorkshire Fire and Rescue Authority as the organisation that determines how data is processed.

Data Processor means any person, other than an employee of the Authority, who processes data on behalf of the data controller, e.g. someone contracted to the Authority to print documents containing personal data.

Data subject is the individual about whom personal data is held.

Personal Data means data about a living individual who can be identified from that information (or from that and other information in the possession of the data controller). This includes an expression of opinion

about the individual, but not any indication of the intentions of the data controller or any other in respect of that individual.

Sensitive Personal Data means personal data consisting of information as to the data subject's:

- Racial or ethnic origin of the data subject
- Political opinion
- Religious beliefs or other beliefs of a similar nature
- Whether they are a Member of a trade union
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of an offence
- Any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings

Processing is very widely drawn and means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including:

- Organisation, adaptation or alteration, disclosure and destruction of the information or data

Relevant Filing System means any manual filing system with an index.

4 Principles

The Data Protection Act 2018 (incorporating GDPR) contains six governing Principles relating to the collection, use, processing and disclosure of data, and the rights of data subjects to have access to personal data concerning themselves. These Principles are:

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

These principles are regarded as the minimum standards of practice for any organisation with respect to personal data.

5 Policy

The Authority supports the objectives of the Data Protection Act 2018 (incorporating GDPR). This policy is intended to maintain the confidentiality of personal data held or processed either on computer or in manual files and to increase the access given to individuals to information relating to them.

The Policy links to the other Authority's policies and procedures:

- Information Security Policy
- Guidance for Managers on the Data Protection Act 2018 (incorporating GDPR)
- Data Protection Act 2018 (incorporating GDPR)Overview and Guidance
- Procedure for dealing with Subject Access Requests
- Records Retention Schedule
- Freedom of Information Policy
- Access to Information Policy

It also links to any Inter-Agency Information Sharing Protocol that the Authority has signed up to.

5.1 External and Internal Registration/Notification

The Authority has an external notification with the Information Commissioner which can be accessed from the Commissioner's website at www.ico.org.uk, and will be supplemented by an internal asset register of data sources and disclosures.

5.2 Fair Obtaining and Processing

West Yorkshire Fire and Rescue Authority will ensure that as far as practicable, all individuals whose details are processed by the Authority are aware of the way in which the information will be obtained, held and disclosed. Processing of personal information by the Authority will be fair and lawful and in addition it is Authority policy that individuals will not be misled as to the purposes for which the Authority will process the information.

5.3 Amount of Data to be Held

The Authority will hold the minimum personal data necessary to enable it to perform its functions. Every effort will be made to ensure that data is accurate and up-to-date, and that inaccuracies are corrected quickly.

5.4 Subject Access

The Authority will provide to any individual who requests it, in a specified manner, a reply stating whether or not the Authority holds personal data about that individual. A written copy, in clear language, of the current data held, will be given, subject to certain exemptions, if specified in the Act.

5.5 Disclosures

Disclosures of information must be, and will be, in accordance with the provisions of the Act, the Authority's notification and the internal register of sources and disclosures. The Authority has a duty to disclose certain data to public authorities such as the Inland Revenue and Customs and Excise. This will be carried out strictly in accordance with the statutory and other requirements.

5.6 System Design

The Authority will ensure that personal data is treated as confidential. Computer systems will be designed and used to comply with the Principles of the Data Protection Act 2018 (incorporating GDPR) so as to ensure that access to personal data is restricted to identifiable system users. The Information Security Policy will apply to this.

5.7 Training

It is the aim of the Authority that all appropriate staff will be properly trained, fully informed of their obligations under the Data Protection Act 2018 (incorporating GDPR) 2018and aware of their personal liabilities.

5.8 Monitoring, Review and Evaluation

The Authority will monitor and review the personal data that it obtains, processes and holds to ensure compliance with the Act. It will maintain a register of all Subject Access Requests made under the Act and the action taken in respect of each application. The Authority will put in place procedures for reviewing its arrangements for administering and handling personal data.

5.9 Disciplinary Action

The Authority expects all of its staff and Members to comply fully with this Policy and the Principles of the General Data Protection Regulations. Disciplinary action may be taken against any employee or Member who breaches any of the instructions or procedures following from this policy.

6 Responsibilities

6.1 The Authority

Overall responsibility for the efficient administration of the General Data Protection legislation lies with the Authority.

6.2 Directors 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 respective Heads of Department for their service area. Within each Department, an Information Champion will be appointed to undertake administration of data protection and to assist in compliance with the requirements of the legislation on behalf of the Chief Legal and Governance Officer or Head of Department and attend the Corporate Information Management Group.

6.3 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 and for checking that those staff understand and appropriately apply policies, procedures and guidance in respect of the Data Protection Act 2018 (incorporating GDPR) in carrying out their day to day work.

6.4 All Staff

It is the responsibility of all staff to process information in accordance with the Data Protection Act 2018 (incorporating GDPR) and to adhere to the policies, procedures and guidance that are laid down by the Authority.

6.5 Information Governance Manager

It is the responsibility of the Information Governance Manager to assist the Authority to ensure compliance with this policy, to specify the procedures to be adopted and to co-ordinate the activities of designated Information Champions.

The main duties of the Information Governance Manager are:

- Maintenance of the Authority's external notification under the Act, and as an interface with the Information Commissioner.
- Development, updating and publication of data protection procedures for the Authority.
- Maintenance of the internal register of data sources and disclosures and to audit data protection procedures and practices.
- Initial contact point for subject access requests.

- In conjunction with the Training Department, the provision of education and training regarding data protection issues.

6.6 Information Governance and Security Group (IGSG)

It is the responsibility of the IGSG to develop and enforce the Information Security Policy for both West Yorkshire Fire and Rescue Authority staff and Members.

6.7 Information Champions

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

- Liaison with the Information Governance Manager on all matters concerning administration of the Act.
- To work with the Director or Head of Department to ensure compliance with the registration particulars in respect to systems within the Directorate.
- To work with the Director or Head of Department to ensure awareness of the Act within the Authority, and to ensure that the control and handling of personal data within the Department or Station does not contravene the Data Protection Principles or Authority procedures.
- Assisting the Information Governance Manager in the collation and validation of external and internal registration particulars relevant to the Authority, and advising the Information Governance Manager of any planned changes to the registration particulars.
- Assisting in the response to access requests from data subjects.

6.8 Officers and Elected Members

In addition to the formal responsibilities outlined above, all Officers and Members have a duty to observe the Principles of the Act and the procedures referred to in this document.

Individuals who do not handle personal data as part of their normal work have a responsibility to ensure that any personal data they see or hear goes no further. This includes personal data and information extracted from such data, thus, for example, unauthorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or even inadvertently by reading a computer screen.

Elected Members will be supplied with personal and sensitive data to enable them to fulfil their duties as Members of committees etc. Members must protect this data and prevent unauthorised or inadvertent disclosure of this data. In terms of data accessed by computer the Information Security Policy will apply.

Disciplinary action may result if the Data Protection Principles or procedures outlined in this document are breached as identified in section 5.9 of this policy.

Elected Members are similar to employees when handling personal data supplied to them by the Authority. In such cases they are not considered to be Data Controllers and have no need to notify the Information Commissioner.

Key Messages

1 This Policy sets out West Yorkshire Fire and Rescue Service's approach to processing personal data under the Data Protection Act 2018 (incorporating GDPR) which attracts the protection of Article 8 of the Human Rights Act 1998.

2 Staff should only collect minimum amount of data which is necessary to enable it to perform its functions.

3 Staff must not share personal third party data with other Fire Service authorities or disclose such data to any other organisation unless they have ensured it is lawful to do so.

4 If West Yorkshire Fire and Rescue Service fail to comply with these rules individuals might be able to claim compensation and the Information Commissioner could fine the Authority up to 20 million Euros.