Service
Policy
Instruction

HEREFORD & WORCESTER
HWFR
FIRE AND RESCUE SERVICE

Data Protection

Folder Name	Management and Administration	Folder Number	1
Section Name	Information Management	Section Number	L
Part Name	Data Protection	Part Number	2

Status	REVISED
Document Version	05.00
Author	B Groom – Data Management Compliance Administrator
SMB Sponsor	J Cole – Head of Corporate Services
Department	Performance & Information
Date Approved	February 2015
Review frequency	2 Years
Next Review	February 2017

Version History		
Version	Date	Description
04.00	Sept 2009	Withdrawn
05.00	Feb 2015	Live

Executive Summary

The Data Protection Act (the Act) 1998 governs the collection, storage, use, disclosure and destruction of personal data, whether held electronically (e.g. in emails, on computer) or in paper/microfiche records.

It applies to all staff who create, store, handle or view personal information held by Hereford & Worcester Fire Authority.

Alternative Formats

If you require this document in another format please contact the Human Resources and Development Department.

Contents

Appendix A

Data Protection

1. Introduction

The Data Protection Act (the Act) 1998 provides a framework to ensure that personal information, whether held on computer or in a manual filing system, is obtained, used, shared and archived / destroyed correctly.

The legislation entitles individuals to know what information is held about them and what it is being used for, the right to request access to personal data, the means to correct, erase and block inaccurate data and in certain instances to claim compensation.

Hereford & Worcester Fire Authority's (HWFA) main priority is to fully comply with the Act and lawfully process data in line with the 8 Data Protection Principles. HWFA must ensure personal data is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to data protection rights
- kept safe and secure
- not transferred outside the UK without adequate protection.

2. Definitions

Data Controller means a person or organisation who determines the purposes and manner in which any personal data are or will be processed.

Data Subject is a living individual to whom personal data relates.

Data Processor means any person (other than an employee of the data controller) who processes the information on behalf of the Data Controller.

Personal Data is data which relates to an identifiable, living individual. Personal information covers recorded facts and any expression of opinion about the individual.

Sensitive Personal Data is a specific term under the Data Protection Act. Sensitive personal data relates to an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or other beliefs of a similar nature
- Membership of trade unions

- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence
- Proceedings for any offence or alleged offence, or court sentence.

There are stringent conditions for managing sensitive personal data which must be complied with prior to any processing taking place.

3. Regulation

The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights and oversee the enforcement and promotion of the Data Protection Act. The ICO has the power to issue Enforcement Notices and monetary penalties of up to £500,000 for serious breaches of data protection law.

4. Notification

HWFA is a Data Controller and is legally obliged to notify its uses of personal data to the ICO on an annual basis, as part of a Register of Data Controllers. The nominated representative for HWFA is the Head of Corporate Services.

5. Training

An on-line "Protecting Information" training programme is being developed for delivery in 2015, to ensure Service staff are trained and fully aware of their Information Security and Data Protection responsibilities. All staff will be required to undertake the training and any subsequent re-fresher sessions. Copies of individual's certificates will be retained by the Service as record of competency.

6. Staff Responsibilities

ALL Fire Authority Members and staff are responsible for complying with the Data Protection Act principles and should follow the Dos and Don'ts list in Appendix A.

7. Disciplinary Action

HWFA expects all Members and staff to comply fully with this Policy and the Information Security Policy. Failure to do so will be viewed as a serious matter and Disciplinary action may be taken.

8. Collecting Personal Data

When collecting personal information, whether from staff or from the public e.g. Home Fire Safety Checks, individuals should be provided with a Privacy Notice or directed to the Service website, for information on how their data will be processed. This includes:

- Who is collecting the data
- Why it is needed
- What it will be used for
- Whether it will be shared with any third party and if so who and for what purpose

It is important to only collect the minimum amount of personal information needed to complete a specific task and the data must be deleted/destroyed when no longer required.

9. Accessing Personal Data (Subject Access Requests)

Individuals have the right to request to view or for copies of their personal information (Subject Access Requests or SARs). All requests for access or assistance should be directed to the Performance & Information Team.

Guidance on how to submit a request is detailed in the Subject Access Request Form (Pers1).

10. Information Sharing

If personal information is to be shared with any other organisation, individuals must be notified of the fact at the point of collection and consent sought. If consent is not provided then personal information must not shared, unless a DPA Exemption applies.

Before any personal information is exchanged, an Information Sharing Agreement between partners / agencies must be undertaken and approved.

11. Data Breaches

Loss or theft of personal information is a serious matter and can have significant consequences both on individuals and on HWFA.

All personal data breaches must be reported to the Head of Corporate Services **immediately.**

Breaches will be managed through the Information Security Policy's incident reporting process and Disciplinary procedures will be instigated where appropriate.

APPENDIX A

Data Protection Act – Staff Dos and Don'ts

DO

- ✔ Where possible inform the individual of the purpose for which you are collecting and using their data, including passing the data onto any third party Privacy Notice
- ✔ Give people the option whether to provide their data or not
- ✔ Make sure when collecting personal data that it is accurate, relevant and not excessive in relation to your needs – make sure you maintain its accuracy
- ✔ Be particularly careful about processing sensitive data: concerning race, political opinion, religious belief, trade union membership, physical or mental health, sexual life, criminal offences
- ✔ Ensure that you have an Information Sharing Agreement in place when sharing personal data with other organisations
- ✔ Recognise a request for personal data and send it to the Performance and Information Team to process
- ✔ Make sure anyone accessing personal information has the right to view it
- ✔ Check recipients contact details are right before providing personal data – always use recorded delivery, if you are not able to hand deliver/collect
- ✔ Make sure any personal data held is kept securely, i.e. kept in a locked filing cabinet or locked drawer, lock workstations when not at your desk
- ✔ Use the Locked Print facility when sending personal data to a shared printer to prevent others from seeing or accidentally collecting your printing
- ✔ Be extra vigilant when working with personal information outside of Service premises. Ensure laptops, memory sticks, tablets, smart phones are encrypted and paper records are kept secure at all times.
- ✔ When disposing of any document containing personal information ensure this is done confidentially (shredder) and in line with the Service's Retention Schedule.
- ✔ Make sure you are familiar with the Service's Information Security Policy

DON'T

- ✘ Process personal data unless you are sure that the individual has given consent or there is a valid legal reason to do so
- ✘ Use personal data collected for one purpose for a different reason without permission from the individual
- ✘ Collect information just for the sake of it
- ✘ Disclose any information (including giving references) about an individual to an external organisation without first checking that the individual has given consent (unless a valid exemption applies)
- ✘ Give personal information out over the telephone
- ✘ Send personal information by fax or use email for confidential communications, as it is relatively insecure
- ✘ Leave personal information unattended and on display i.e. don't leave personal information on the Fire Appliance or in a Fire Safety vehicle, don't leave your PC unlocked when away from your desk, don't leave information on your desk when you leave at night
- ✘ Write any comment about any individual that is unfair or untrue and that you would not be able to defend if challenged. You should assume that anything that you write about a person may be seen by that person
- ✘ Keep information once you have finished with it just in case and make sure it is disposed of securely

Think before you act, use common sense and if in doubt seek advice or guidance