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	REVIEW
Document Version	07.07
Author	Information Governance Officer
SLB Sponsor	Head of Legal Services
Directorate	Legal Services
Date Approved	23/05/2023
Review frequency	2 Years
Next Review	23/05/2025

Version History		
Version	Date	Description
04.00	Sept 2009	Published
05.00	February 2015	Revised and Published
06.00	February 2016	Revised and Published
07.00	February 2018	Revised and Published
07.06	Aug 2018	GDPR revision
07.07	23/05/2023	Update

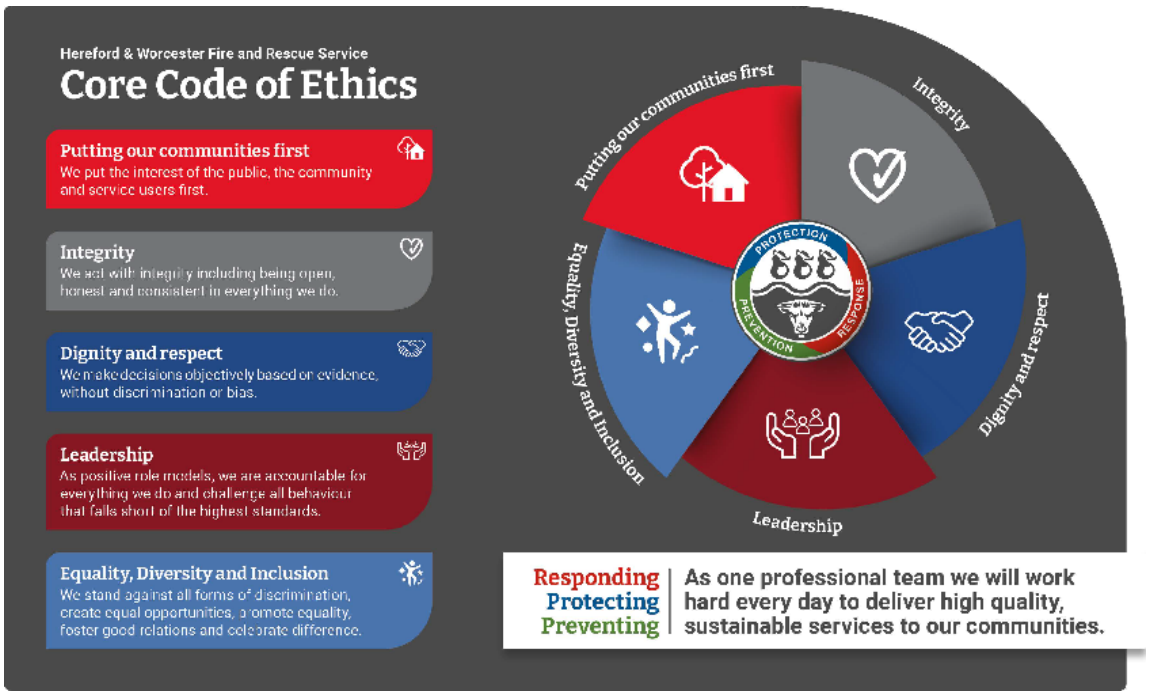
Executive Summary

The UK General Data Protection Regulation (GDPR) substantially re-enacts the previous data protection regime applicable as part of the European Union (EU). It includes obligations and requirements for the collection, storage, use, disclosure and destruction of personal data, in all formats e.g. in the cloud, emails, on computer, paper, microfiche records.

It applies to all staff who create, store, handle or view personal information held by Hereford & Worcester Fire and Rescue Service (HWFRS).

Core Code of Ethics

The Core Code of Ethics for Fire and Rescue Services in England sets out five ethical principles, which provide a basis for promoting good behaviour. The Service is committed to the ethical principles of the Code and used them as guidance when forming Service's values. The principles of the Code are reflected in this policy as well.



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

1.1 Data protection is governed by the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

1.2 Data protection (DP) core functions remain the same, providing an assurance framework for how personal information is managed, obtained, used, shared and archived / destroyed, whether held electronically or in a hard copy format.

1.3 GDPR governs the ways that information is collected and used and contains rights for individuals, giving them control over what happens to their information. It also allows for significant financial penalties to be imposed on any organisation in breach of the Regulation.

2. Principles

2.1 There are seven general principles under the GDPR (Article 5):

- Personal information shall be processed lawfully, fairly and in a transparent manner.
- Personal information shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Personal information shall be adequate, relevant and limited to just sufficient to complete the task.
- Personal information shall be accurate and, where necessary, kept up-to-date.
- Personal information shall be retained only for as long as necessary.
- Personal information shall be processed in an appropriate manner to maintain security.
- The controller should be accountable for what happens to the personal information and how they comply with the other principles

2.2 This Policy applies to staff, volunteers, contractors and visitors, who are responsible for complying with Data Protection principles and should follow the Dos and Don'ts list in Appendix A.

3. Definitions

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

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

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

3.4 **Personal data,** under GDPR Article 4, is any information that relates to an identifiable, living individual (data subject) who can be identified, directly or indirectly, by an identifier such as:

- a name, email address, phone number
- personal identification numbers, e.g. staff number, bank account, national insurance number
- aspects specific to an individual's physical, physiological, genetic, mental, economic, cultural or social identity.
- location data - data that has any kind of geographic position attached to it, e.g. data collected by wireless networks, swipe cards and smart mobile devices that provide location tracking
- online identifiers, e.g. mobile device IDs, browser cookies, IP addresses

3.5 Personal data may only be lawfully processed under GDPR Article 6(1) when one or more of the following requirements are met:

- Consent has been freely given
- Necessary for a contract
- To comply with a legal obligation
- To protect the vital interests of a data subject or another person
- Tasks carried out in the public interest
- For legitimate interests – NB, Public Authorities including the Service, cannot rely upon this reason

3.6 Particularly **special** (sensitive) **categories of personal data** which relate to an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Membership of trade unions
- Genetic data / biometric data
- Physical or mental health or condition
- Sex life or sexual orientation

may only be processed if a lawful reason can be identified under GDPR Article 6(1) **and** an additional reason is met as well under GDPR Article 9:

- Explicit consent has been freely given

- Necessary for the carrying out of employment, social security or social protection law
- Necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent
- Processing relates to members or former members carried out by not-for-profit bodies with political, philosophical, religious or trade union aims
- Personal information is made public by the individual
- Needed for the establishment, exercise or defence of legal claims or for judicial capacity of the courts
- Necessary for reasons of substantial public interest
- Required for the purposes of preventative or occupational medicine
- Public interest in public health
- Needed for archiving in the public interest, scientific, historical or statistical purposes.

3.8 When personal data is needed for criminal investigations, convictions or offences, not only must a lawful basis under Article 6 (Section 3.5 above) be identified but also an additional reason under Article 10 - Processing of personal data relating to criminal convictions and offences.

3.9 When processing special category personal data for criminal convictions, employment, health, research or in substantial public interest cases, then DPA 2018 Schedule 1 must be taken into consideration along with GDPR Articles 9 and 10.

4. Handling Personal Data

The Service relies upon quality information in order to successfully deliver an effective emergency service; whether that is attending the correct address at an incident, providing smoke alarms to the right recipients at a Home Fire Safety Check or ensuring that staff receive the right support from Occupational Health when needed.

It is important that all Service information is handled appropriately but specific care and attention must be paid when processing personal and special personal data (sections 3.4 and 3.6). These data types must only be processed by staff when they have a legitimate reason to access and when the conditions set out in sections 3.5 and 3.7 are met.

All staff are required to complete appropriate training to ensure competency on recognising / identifying personal data and understanding how and when it should be used. A brief “Do’s and Don’ts” on managing personal data is detailed in Appendix A and further guidance is available on the Information Governance SharePoint page.

5. Regulation

The Information Commissioner's Office (ICO) is the UK’s lead authority overseeing personal information rights. The ICO has the authority to issue warnings of non-compliance, carry out

audits, require specific remediation within a specified time frame, order erasure of data and issue substantial monetary penalties for serious breaches of data protection law.

6. Data Protection Registration

Under the UK GDPR, the requirement to inform (notify) the ICO why personal data is being processed, has been abolished. From May 2018, the ICO will instead collect and publish:

- the name and address of the data controller
- the data protection registration number issued by the ICO
- any applicable fee
- date fee paid and expiry date
- contact details for the individual responsible for DP within HWFRS.

Registration fees will be implemented through the Digital Economy Act 2017, rather than GDPR and divided into tiers 1 – 3, with HWFRS fitting into tier 3, with fees set at £2900.00.

7. Accountability

GDPR has a specific accountability principle (Article 5(2)) that requires the HWFRS to actively demonstrate and record how compliance with the DP principles are met and maintained.

A key point to establishing compliance is by embedding privacy standards at the very beginning of all new programmes and projects that require the processing of personal data.

A Data Protection Impact Assessment (DPIA) is a process designed to help identify and minimise the data protection risks of a project. A DPIA must:

- describe the nature, scope, context and purposes of the processing
- assess necessity, proportionality and compliance measures
- identify and assess risks to individuals
- identify any additional measures to mitigate those risks.

This “data protection by design and default” approach will help to reduce the likelihood of having to implement expensive, cumbersome and time consuming DP “bolt-on” measures during the project’s lifespan.

8. Data Protection Officer

It is compulsory under GDPR for public authorities, to appoint a named Data Protection Officer (DPO).

DPOs are required to inform and advise on data protection obligations to Senior Management, monitor compliance and provide advice regarding completing Data Protection Impact Assessments (Refer to Section 6).

DPO’s must have the full support of Senior Management, be totally impartial and cannot undertake any other function which may lead to a conflict of interests.

It is essential that DPOs have an expert knowledge of UK and European data protection laws, undertake continuous training and act as the first point of contact for members of staff, public and for the ICO. The DPO does not have to be a member of staff and the function can be contracted out. The Service has therefore chosen to appoint Aristi Limited as it's Data Protection Officer. Any enquiries or requests for advice should be directed to the Information Governance Officer or Head of Legal Services in the first instance, who will then contact Aristi Limited as necessary.

9. Privacy Notices

GDPR requires a Privacy Notice to be given to the individual supplying personal information, that explains:

- Who the Data Controller is and their contact details
- The purpose of processing and legal basis for doing so
- Who the information will be shared with if applicable e.g. other Fire and Rescue Services / Partners / Police etc.
- How long the information will be kept for (retention period)
- How to withdraw consent for processing (refer to 10)
- How to request a copy of their information and for it to be amended if incorrect
- How to request their data to be deleted
- Who to contact with a complaint and how to contact the ICO if the issue is not resolved internally.

The Privacy Notice should be given at the point of information collection, however where this is not possible or involves a disproportionate effort e.g. at an incident, people should be informed that Privacy Notices are available on HWFRS' website. 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.

10. Individual's Rights

GDPR establishes a specific set of data subject's rights relating to their personal data:

1. The right to be informed

Data subjects must be provided with a minimum of information regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

2. The right of access (subject access requests)

Data subjects have the right to obtain a copy of their personal data, together with an explanation of the categories of data being processed, the purposes of such processing, who the data will be shared with as well as details of the period for which the data will be retained.

Information on how to submit a request for personal data is detailed in Pers 1 – Subject Access Request Form.

3. The right to rectification

Data subjects are entitled to have personal data rectified if it is inaccurate or incomplete. Staff are required to take reasonable steps to ensure that their personal data held by the HWFRS is correct, by checking and updating HRConnect as necessary. Queries should be emailed to HRSupport@hwfire.org.uk.

4. The right to erasure

Data subjects have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The Service can refuse such requests if there are legitimate reasons why the data still needs to be retained.

5. The right to restrict processing

Data subjects have a right to object to specific types of processing:

- Direct marketing
- Processing based on legitimate interests or performance of a task in the public interest/exercise of official authority
- Processing for research or statistical purposes

6. The right to data portability

Data subjects are entitled to receive a copy of their personal data in a commonly used machine-readable format and to transfer their personal data from one data controller to another or have the data transmitted directly between data controllers.

7. The right to object

Data subjects have the right to object to the processing of their personal data based on the performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling) and processing for purposes of scientific/historical research and statistics.

8. Rights in relation to automated decision making and profiling

Data subjects have the right not to be subject to decisions based solely on automated processing which significantly affect them. Where such an automated decision has been made the data subject has a right to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

11. Consent

GDPR clarifies the situation of consent for the processing of personal data.

Consent must be unambiguous, informed and feely given, leaving no doubt as to wishes of the data subject. If consent is being relied on to process personal data, rather than another lawful reason, there must be a genuine opportunity for an individual to refuse, with an "opt-in" rather than "opt-out" choice: GDPR specifically bans pre-ticked opt-in boxes. In all instances, the fact that consent has been given must be recorded.

Individuals must be informed that they can withdraw their consent to processing at any time and be provided with details of how to request this. A Privacy Notice (refer to Section 8) should always be given when collecting personal data.

12. Children

Children need particular protection when collecting and processing their personal data because they may be less aware of the risks involved. Fairness is a key GDPR data protection principle when processing children's data

If relying on consent as the lawful basis for processing (refer to Section 10), children aged 13 or over are able provide their own consent. For children under this age, consent is needed from whoever holds parental responsibility for the child.

Children have exactly the same rights as adults over their personal data, as defined in Section 9 and require a clear privacy notice (refer to Section 8) written in plain, age-appropriate language, explaining what will happen to their personal data and their rights.

13. Exemptions

There are exemptions (derogations) to an individual's rights under GDPR; however they must be proportionate and still take into account a Data Subject's fundamental rights and freedoms.

Exemptions apply to:

- national security
- defence
- public security
- the prevention, investigation, detection or prosecution of criminal offences
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security
- the protection of judicial independence and proceedings
- breaches of ethics in regulated professions

- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention
- the protection of the individual or the rights and freedoms of others
- the enforcement of civil law matters.

Staff must not attempt to reply to requests for personal information themselves. All requests for personal data need to be sent to the Information Governance Officer in the first instance to ensure that they are logged and responded to appropriately. This includes considering whether there are any relevant exemptions and applying them as necessary.

14. Training

All staff are required to undertake e-Learning "Protecting Information" training appropriate to their role and level of exposure to personal data, to ensure they are fully aware of their Information Security and Data Protection responsibilities.

Staff will be contacted concerning refresher training sessions which will be run on a bi-annual basis.

15. Data Breaches/Information Security Breaches

The loss or theft of personal information can have significant consequences both on individuals and on HWFRS. There must be appropriate technical and organisational measures in place in order to process personal data, as detailed in the Information Security Policy Framework.

If a serious breach does occur, the GDPR sets a time limit of 72 hours to inform the ICO and therefore all personal data breaches must be reported to Fire Control **immediately upon discovery** using the Information Security Incident Management Policy.

Reporting a breach or a potential breach (near-miss) can help to reduce the harm to an individual and the impact on the organisation. It can also help to prevent future infringements and should not be regarded negatively but encouraged as best practice for future learning opportunities.

All breaches will be routinely investigated and where there has been a deliberate misuse or theft of personal data, disciplinary proceedings may be actioned.

16. Information Sharing

If personal information is to be shared with any other organisation, an Information Sharing Agreement must be drafted and approved before any data is exchanged. Individuals must be informed that their data may be / will be shared with another party when their data is being collected.

If consent is being relied upon, data subjects can refuse for their information to be shared and in such cases, personal information must not be disclosed. Refer to Section 10.

If there is another lawful reason for collecting, using and sharing the data e.g. to protect the vital interests of the data subject or another individual, then information may be shared without consent.

17. International Transfers

No personal data may be transferred outside of the EEA without approval of the Head of Legal Services or Senior Leadership Board (SLB). This includes using cloud based services which are hosted outside of the EEA.

In all such instances a DPIA must be completed and advice sought from the Information Governance Officer or Head of ICT before transferring any data.

18. Monitoring and Assurance

Compliance with data protection legislation will be monitored through a programme of audits undertaken by the Information Governance Officer.

APPENDIX A

Data Protection – Staff Dos and Don'ts

DO

- ✓ Complete a Data Protection Impact Assessment before starting any new project or programme that involves personal data.
- ✓ Where appropriate, issue the individual with a Privacy Notice explaining why you are requesting and using their data, at the time you are collecting the information
- ✓ Give people the genuine 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 special (sensitive) data concerning race, political opinion, religious belief, trade union membership, physical or mental health, sexual life, criminal offences – always consider whether you really need to have this information and how you are going to ensure it is kept safe and only shared with those who have a legitimate reason to access it
- ✓ Ensure that you have an Information Sharing Protocol Agreement in place before sharing personal data with other organisations
- ✓ Recognise a request for personal data (subject access request) and send it to theinformationrequests@hwfire.org.uk– do not attempt to answer these requests yourself
- ✓ Make sure anyone wanting access to personal information is permitted to do so before you provide any details
- ✓ Check recipients contact information is right before providing personal data – check pre-populated email addresses before you send and 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 "Follow-Me" 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 HWFRS 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 HWFRS' Records Management Policy and Information Disposal Policy
- ✓ Make sure you are familiar with HWFRS' Information Security Policy Framework

DON'T

- ✘ Process personal data unless you are sure that the individual has given their consent / explicit consent or if there is another valid legal reason to do so (sections 3.5 and 3.7)
- ✘ Use personal data collected for one purpose for a different reason without permission from / notifying the individual
- ✘ Collect just for the sake of it or "just in case"
- ✘ 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 or in an area where you can be overheard
- ✘ 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
- ✘ Retain duplicate copies of personal information once the original record has been submitted to the relevant Department / Station for filing.
- ✘ Keep information once you have finished with it on a "just in case" basis and make sure it is disposed of securely

Think before you act, use common sense and if in doubt seek advice and guidance from the Information Governance Officer.