Service
Policy /
Instruction

HEREFORD & WORCESTER HWFR FIRE AND RESCUE SERVICE

Data Protection

Status	LIVE
Document Version	Version 7.09
Author	Information Governance Officer
SLB Sponsor	Area Commander Prevention
Directorate/ Department	Prevention
Date Approved	15/09/2025
Review frequency	2 Years
Next Review	15/09/2027

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
07.08	09/05/2025	Revised and Published
07.09	**15/09/2025**	**Addition of Data (Use and Access) Act 2025**

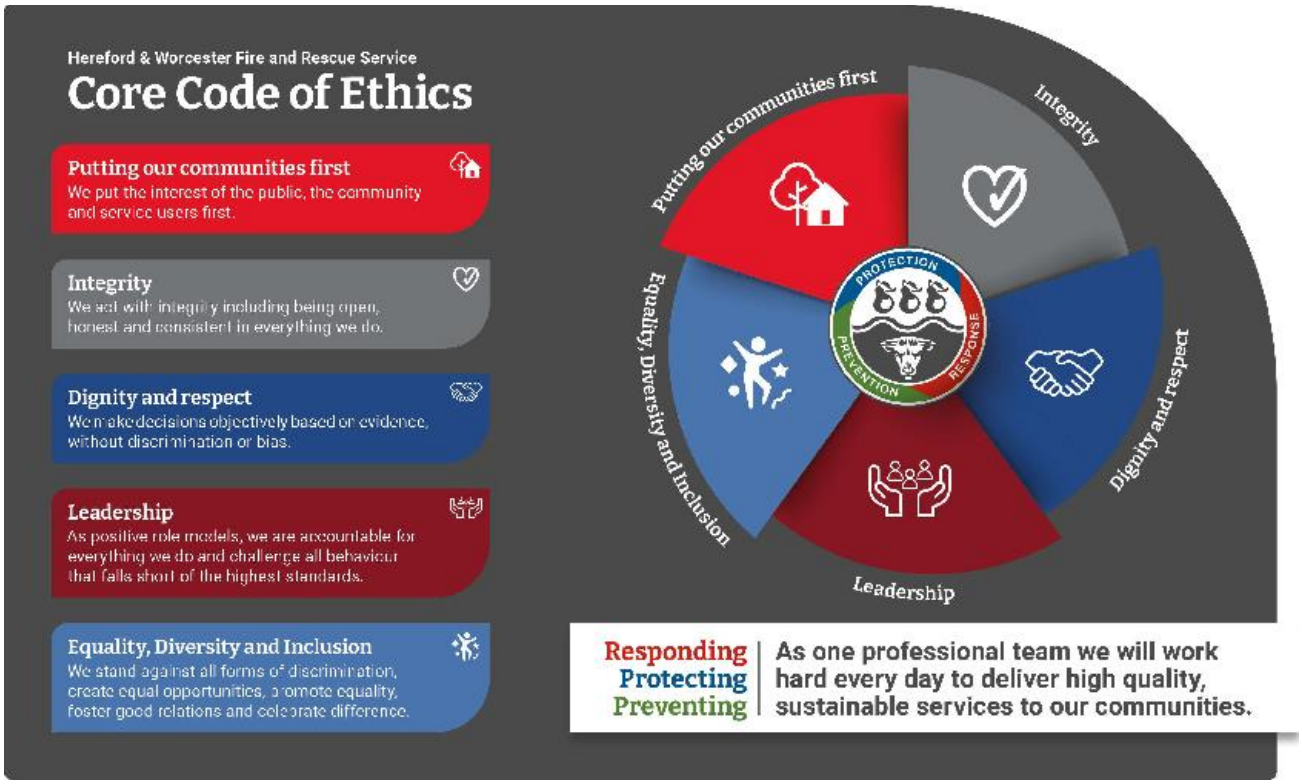
Executive Summary

The UK General Data Protection Regulation (UK 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 sets out five ethical principles, which provide a basis for promoting good behaviour and challenging inappropriate behaviour. The Service is committed to the ethical principles and professional behaviours contained in the Core Code of Ethics, which sets expectations on governance, behaviour and integrity in the Fire Sector. The principles of the Code are reflected in this policy as well.



Safeguarding Policy Statement:

Safeguarding is everyone's responsibility, and Hereford & Worcester Fire and Rescue Service (HWFRS) are committed to safeguarding children, young people and adults from abuse and neglect. The Service strives to promote the safety, dignity and wellbeing of staff and people in the community.

Safeguarding practices within HWFRS align to the Safeguarding Fire Standard which aims to ensure that Service support and promote the safeguarding of those within the community, employees and volunteers. Safeguarding - Fire Standards Board

All HWFRS staff will adhere to the Service's Adult Safeguarding Policy and Children and Young People Safeguarding Policy and associated Guidance.

SPIs (sharepoint.com)

Alternative Formats

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

Data Protection

1. Introduction

1.1. Data Protection is governed by the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data Use and Access Act 2025.

1.2. These provisions provide an assurance framework for how personal information is obtained, managed, used, shared and archived / destroyed, whether held electronically or in a hard copy format.

1.3. The UK GDPR governs the ways that information is collected and used and contains rights for individuals, giving them a measure of 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 UK 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 what is necessary 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 data 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 the UK 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 the UK GDPR Article 6(1) when one or more of the following requirements are met:

- Consent has been freely given
- It is necessary for a contract
- It is to comply with a legal obligation
- It is to protect the vital interests of a Data Subject or another person
- It is for a task carried out in the public interest
- To further legitimate interests – NB, Public Authorities, including the Service, cannot rely upon this reason in circumstances where the public interest ground could be used instead

3.6 Particularly sensitive types of personal data (known as Special Category) that 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 the UK GDPR Article 6(1) **and** an additional reason is met under the UK GDPR Article 9(2):

- Explicit consent has been freely given
- It is necessary for discharging obligations & rights under employment, social security or social protection law
- It is necessary to protect the vital interests of a living person who is physically or legally incapable of giving consent

- The processing relates to members or former members of not-for-profit bodies with political, philosophical, religious or trade union aims, carried out in the body's legitimate interests.
- The personal information is made public by the Data Subject
- It is needed for the establishment, exercise or defence of legal claims or for the judicial capacity of the courts
- It is necessary for reasons of substantial public interest
- It is required for the purposes of preventative or occupational medicine, health and social care or assessing an employee's working capacity.
- It is necessary for the public interest in the area of public health
- It is needed for archiving in the public interest, scientific, historical or statistical purposes.

3.7 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 an additional reason under Schedule 1 of the DPA 2018 must also be met.

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 it 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 (See Section 14 below). 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 regulatory 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

All organisations processing personal data must register with the ICO. The ICO will collect and publish:

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

Registration is divided into three tiers. HWFRS fits into tier 3, with fees set at £3763.00.

7. Accountability

The UK 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 “bolt-on” DP measures during the project’s lifespan.

8. Data Protection Officer

It is compulsory under the UK 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 7).

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 interest.
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, the 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 Ltd as its 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 as necessary.

9. Privacy Notices

Article 13 of the UK GDPR requires a Privacy Notice to be given to the individual whose personal information is being processed. This Privacy Notice must explain:

- Who the Data Controller is and their contact details
- The purpose of the 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 Section 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 cannot be resolved internally to the individual's satisfaction.

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. Individuals' Rights

The UK GDPR establishes a specific set of Data Subjects' rights as relates 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 (See Section 9).

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 HR Connect 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 request that their information be retained but not otherwise processed by the Service except by consent, for legal claims, for the protection of rights or for reasons of important public interest. They can request restriction where:

- Accuracy of the information is being contested by the Data Subject and is being verified by the Service
- The Data Subject has exercised their right to object and the Service is verifying whether its grounds for holding the information overrides the Data Subject's
- The processing has been found to be unlawful but the Data Subject wants the information retained rather than erased
- The Service no longer needs the information but the Data Subject needs it for use in legal claims

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 in order to transfer that data to another data controller or to 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 or legitimate interest (including profiling) and processing for purposes of scientific/historical research and statistics. The Service can refuse such requests if there are legitimate reasons why the data still needs to be retained that override the Data Subject's interests or if the information is needed for legal claims.

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, obtain an explanation of the decision and challenge it.

11. Consent

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

Consent must be unambiguous, informed and freely 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: The UK 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 9) should always be given when collecting personal data.

Consent is only one possible legal basis for processing personal data and several others are available (See Section 3.5)

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 UK GDPR data protection principle when processing children's data

If relying on consent as the lawful basis for processing (refer to Section 11), 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. However, a child can override a parent's request for their information.

Children have exactly the same rights as adults over their personal data, as defined in Section 10 and require a clear privacy notice (refer to Section 9) written in plain, age-appropriate language, explaining what will happen to their personal data and their rights.

13. Exemptions

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

Exemptions apply to, among others:

- 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 'GDPR' training on the LMS that is 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 an annual basis.

15. Data Breaches / Information Security Incidents

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 ICT Security Policy Framework.

If a serious breach does occur, the UK 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 to allow 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. For example, in the case of multi-agency emergency response situations such as flooding, the Civil Contingencies Act 2004 (Contingency Planning) Regulations 2005 allows responders to share information to aid with the emergency response

17. International Transfers

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

In all such instances a DPIA must be completed and advice sought from the Information Governance Officer and the 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 Data Subject 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 category (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 Agreement in place before sharing personal data with other organisations
- ✔ Recognise a request for personal data (Subject Access Request) and send it to informationrequests@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 signed for 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
- ✔ 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' ICT Security Policy Framework

DON'T

- ✘ Process personal data unless you are sure that the individual has given their 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 personal data 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 a 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. 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.

HEREFORD & WORCESTER HWFR FIRE AND RESCUE SERVICE

No: 76

Appendix 1

People Impact Assessment (PIA)

Policy / Project / Function:	Data Protection				**Date of Assessment:**		09/05/2025 06/06/2023			
Analysis Rating: please tick 1 box ✓ *(The analysis rating is identified after the analysis has been completed - See Completion Notes).*	**RED**		**AMBER**		**GREEN**	✓	Proportionate means achieving a legitimate aim/can be objectively justified.		**Action Plan included?**	

Please list methods used to analyse impact on people (e.g. consultations forums, meetings, data collection)	Performance Report Quarter Q3 2024 to 2025 Office for National Statistics Census for Worcestershire 2021 Office for National Statistics Census for Herefordshire 2021
Please list any other policies that are related to or referred to as part of this analysis	ICT Policy Framework Information Security Incident Management Policy Overarching Information Sharing Policy
Please list the groups of people potentially affected by this proposal. (e.g. applicants, employees, customers, service users, members of the public)	Employees, Applicants & Service Users

What are the aims and intended effects of this proposal (project, policy, function, service)?

To inform and promote awareness of the Data Protection protections and obligations that the Service is bound by; providing clarification on what personal data is and how it is handled, stored, the reasons for its use and how long it will be retained.

This policy has been produced in line with statutory provisions and the Information Commissioner's Office's guidance.

Is any Equality Data available relating to the use or implementation of this proposal (policy, project, or function, service?)
Please Tick ✓(See Completion notes)

YES:	**NO:** ✓

List any Consultations e.g. with employees, service users, Rep Bodies or members of the public that has taken place in the development or implementation of this proposal (project, policy, function)?

All policies undergo a comprehensive internal consultation process.

People Impact Assessment (PIA)

Appendix 1

What impact will the implementation of this proposal have on people who share characteristics protected by *The Equality Act 2010*? Please Tick ✓(See Completion notes)				
Protected Characteristic:	**Neutral Impact:**	**Positive Impact:**	**Negative Impact:**	**Evidence of impact and if applicable, justification if determining proportionate means of achieving legitimate aims exists**
Sex (Men and Women)	X			Neither a positive nor negative impact has been identified for this protected characteristic
Race (All Racial Groups)	X			Neither a positive nor negative impact has been identified for this protected characteristic
Disability (Mental, Physical, and Carers of Disabled people)	X			Neither a positive nor negative impact has been identified for this protected characteristic
Religion or Belief	X			Neither a positive nor negative impact has been identified for this protected characteristic
Sexual Orientation (Lesbian, Gay, Bisexual and Straight)	X			Neither a positive nor negative impact has been identified for this protected characteristic
Pregnancy and Maternity	X			Neither a positive nor negative impact has been identified for this protected characteristic
Marital Status (Married and Civil Partnerships)	X			Neither a positive nor negative impact has been identified for this protected characteristic
Gender Reassignment (Includes non-binary)	X			Neither a positive nor negative impact has been identified for this protected characteristic
Age (People of all ages)	X			Neither a positive nor negative impact has been identified for this protected characteristic

What impact will the implementation of this proposal have on people who are impacted by and / or local factors that sit outside the Equality Act 2010 (non-legislative). Examples include social economic factors (i.e. poverty and or isolation), caring responsibility, unemployment, homelessness, urbanisation, rurality, health inequalities, any other disadvantage. ✓ (See Completion notes)				
Identified impact non-legislative factor	**Neutral Impact:**	**Positive Impact:**	**Negative Impact:**	**Evidence of impact and if applicable, justification if determining proportionate means of achieving legitimate aims exists**

Initial People Impact Analysis completed by: (Name & Dept/Stn): Lorraine Adams – Legal Services…….. **WHEN PIA REVIEWED** - Reviewed by: Alex Wooding - Prevention
Review Date: 08/05/25

Please see 'Notes for PIA Authors' below

Action Plan Owner:	**Commencement date:**	**Sign off date:**

As a result of performing this analysis, what actions are proposed to remove or reduce any negative impact of adverse outcomes identified on people (employees, applicants, customers, members of the public etc) who share characteristics protected by *The Equality Act 2010* or are non-legislative characteristics?

Action Planning

Identified Impact Protected Characteristic or local non-legislative factor	**Recommended Actions**	**Responsible Lead**	**Completion Date for Any Actions Listed**
Overall	To ensure the policy is clear on the handling of data and up to date with the latest legislation	Information Governance Officer	In line with policy review
Local non-legislative factors	All data to be kept up to date and accurately recorded	Managers of each department	Every 3 months

Notes for PIA Authors:

- People Impact Assessments should be reviewed whenever a policy/project/function is reviewed.
- If there are (1) only minor alterations to a policy/project/function, (2) the existing PIA has already been quality assured, and (3) the author feels the minor changes don't affect the findings detailed in the PIA, there is no need for it to be quality assured once again. The PIA should have a new date on Page 1 showing when it was last reviewed.

Document quality assured by & Date: ……K L Berry, EDI Officer – 06/06/23……
(Quality assured by appropriate person, eg EDI Officer, Inclusion & OD Manager)

Completion Notes:	
Analysis Ratings:	The analysis rating is located at the top of the document so that if you have several impact assessments you will be able to determine priority impact status. To assure the assessment determines the rating, the rating should not be determined before the assessment has been completed. **Red:** As a result of performing this assessment, it is evident a risk of discrimination exists (direct, indirect, unintentional, or otherwise) to one or more of the nine groups of people who share Protected Characteristics (and / or local non-legislative factors). In this instance**, it is recommended that the use of the activity or policy be suspended** until further work or analysis is performed. If it is considered this risk of discrimination (is objectively justified, and/or the use of this proposal (policy, activity, function) is a proportionate means of achieving a legitimate aim; this should be indicated and further professional advice taken. **Amber:** As a result of performing this assessment, it is evident a risk of discrimination (as described above) exists and this risk may be removed or reduced by implementing the actions detailed within the *Action Planning s*ection of this document. **Green:** As a result of performing this assessment, no **adverse effects** on people who share Protected Characteristics and/or local non-legislative factors are identified - no further actions are recommended at this stage. (However, there may still be actions listed in the *Action Planning* section, reinforcing positive outcomes).
Equality Data:	Equality data is internal or external information that may indicate how the activity or policy being analysed can affect different groups of people who share the nine Protected Characteristics and / or local non-legislative factors. Examples of Equality Data include: (this list is not definitive) 1: Application success rates by Equality Groups 2: Complaints by Equality Groups 3: Service usage and withdrawal of services by Equality Groups 4: Grievances or decisions upheld and dismissed by Equality Groups
Legal Status:	This document is designed to assist organisations in *"Identifying and eliminating unlawful Discrimination, Harassment and Victimisation"* as required by The Equality Act Public Sector Duty 2011. The NFCC/FRSs may be keen to extend "due regard" to local/non-legislative factors such as social economic factors (i.e. poverty and or isolation), caring responsibility, unemployment, homelessness, urbanisation, rurality, health inequalities any other disadvantage. ✔ (See Completion notes). **What impact will the implementation of this proposal have on people for which there is no legal requirement**? (consider each local non-legislative factor separately). Doing this analysis may also identify opportunities to *foster good relations* and *advance opportunity* between those who share Protected Characteristics and / or local non-legislative factors and those that do not. *An EqIA is not legally binding and should not be used as a substitute for legal or other professional advice.*
Objective and/or Proportionate	Certain discrimination may be capable of being defensible if the determining reason is: (i) *objectively justified* *(ii) a proportionate means of achieving a legitimate aim* of the organisation For *objective justification*, the determining reason must be a real, objective consideration, and not in itself discriminatory. To be *'proportionate'* there must be no alternative measures available that would meet the aim without too much difficulty that would avoid such a discriminatory effect. Where (i) and/or (ii) is identified it is recommended that professional (legal) advice is sought prior to completing an People Impact Assessment.

Appendix 2

Organisational Impact Assessment

1. Preliminary Questions:			
Policy, Project or Activity:	Data Protection	Author:	Alex Wooding
Department:	Prevention	Title:	Information Governance Officer
New /existing?	Existing	Date:	09/05/2025
2. Information on the Policy, Project or Activity:			
How does the Policy, Project or Activity fit in with our core purpose and strategies?	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		
3. Are there any implications for the following? If yes, please provide brief description:			
Operational	Will sometimes need to handle sensitive personal information during operations		
Legal	Keeping abreast of changes in legislation that may affect this policy in future.		
Human Resources	Store and handle more personal data of all kinds than any other department. Must be careful to safeguard that information.		
Training and Development	Must provide ongoing Data Protection training to all staff.		
ICT	Obligations to safeguard personal data emphasises cybersecurity		
FRA	No		
Resource	No		
Service Delivery	No		
Consultation with Rep Bodies	Trade Union membership is considered sensitive personal data		
Corporate Communications	Avoid publishing sensitive personal data		
Health and Safety	Will handle sensitive health information that must be safeguarded		
Sustainability	No		
Partnership Working	No		
Other Implications/ Considerations?	All staff must be careful not to commit data breaches, e.g. by sending emails to the wrong recipients.		

4. What are the risks in carrying out / delivering the activity described?

Consider: financial, reputational, environmental, health and safety, information management etc.
N.B. Please make your SLB member aware of any significant risks for elevation to their Risk Register.

No.	Risk	Risk			Potential control measures	Residual Risk			Outstanding exposures
		Likelihood	Impact	Risk Score		Likelihood	Impact	Risk Score	
1	**Information Management**	**4**	**3**	**12**	**Adhering to SPI and Legislation**	**2**	**2**	**4**	**Human Error**
2	**Reputational**	**3**	**4**	**6**	**Adhering to SPI and Legislation**	**1**	**3**	**3**	**Human Error**

Please use the matrix below to assess likelihood and impact:

IMPACT	Severe (5)	5	10	15	20	25
	Major (4)	4	8	12	16	20
	Moderate (3)	3	6	9	12	15
	Minor (2)	2	4	6	8	10
	Minimal (1)	1	2	3	4	5
		Low (1)	Low/ Medium (2)	Medium (3)	Medium/ High (4)	High (5)
	LIKELIHOOD					

5. Data Protection

A Data Protection Impact Assessment (DPIA) will assist in identifying and managing any project privacy implications and risks; for example, when making significant changes to existing practice, when developing a new project or when changing suppliers or processors.

The Screening Questions below are intended to help identify whether a DPIA is required. Answering '**Yes**' to any of these questions indicates that a DPIA is necessary.

Screening Questions	***Yes/No***
Will the policy, project or activity involve the collection of new information about individuals?	No
Will the policy, project or activity compel individuals to provide information about them?	No
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	No
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No
Does the policy, project or activity involve you using new technology that might be perceived as being privacy intrusive? For example, recording images, biometrics or facial recognition.	No
Will the policy, project or activity result in your making decisions or taking action against individuals in ways that can have a significant impact on them?	No
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	No
Will the policy, project or activity require you to contact individuals in ways that they may find intrusive?	No

You will find a DPIA template and guidance notes on the Information Governance SharePoint page. Follow the link and click on 'DPIA Instruction' - Information Governance**.**

If you require any assistance in completing the data protection impact assessment or need further guidance, contact the Information Governance Officer on informationrequests@hwfire.org.uk