HUMBERSIDE FIRE AND RESCUE SERVICE

People & Culture

Firewatch Policy

Owner	**Assistant Director of People & Culture**
Responsible Person	**Head of Human Resources**
Date Written	**October 2025**
Date of last review	**October 2025**
Date of next review	**October 2028**
EIA Completed	**October 2025**

CONTENTS

1. POLICY STATEMENT AND INTRODUCTION

The policy applies to all employees and users of the FireWatch software and is to be used in conjunction with other service polices such as the Data Protection Policy and the Information Security policy

FireWatch is a cloud hosted People and Availability software system that manages and maintains the establishment and availability of HFRS staff. It holds and keeps personnel records, monitors and manages staff availability, and connects to the Command & Control system that mobilises appliances to incidents within the community area we serve.

The system is driven by data, and it is the integrity and availability of this data that is paramount to it performing the function it has been procured for.

The system is solely reliant on the data it contains, and people make decisions based on that data. It is crucial that data quality and accuracy is managed and maintained at all times.

The Head of People & Culture has ultimate responsibility for the FireWatch system, supported by the full people team, ensuring that the information held within, is accurate, relevant and timely.

It is also everyone's responsibility to ensure that personal data that is held within the FireWatch system is also accurate. This included details such as name, contact details, emergency contact information, secondary employment, date of birth, national insurance number etc.

Core Code Of Ethics

Humberside Fire & Rescue Service (HFRS) has adopted the Core Code of Ethics for Fire and Rescue Services. The Service is committed to the ethical principles of the Code and strives to apply them in all we do; therefore, those principles are reflected in this Policy.

National Guidance

Any National Guidance relating to the management of data that has been adopted by HFRS will be reflected in this Policy.

2. EQUALITY, DIVERSITY AND INCLUSION

HFRS has a legal responsibility under the Equality Act 2010, and a commitment, to ensure it does not discriminate either directly or indirectly in any of its functions and services or in its treatment of staff, in relation to race, sex, disability, sexual orientation, age, pregnancy and maternity, religion and belief, gender reassignment or marriage and civil partnership. It also has a duty to make reasonable adjustments for disabled applicants, employees, and service users.

3. AIM AND OBJECTIVES

The FireWatch system and the data held within, must be secure, accurate, relevant, and when needed, updated in a timely manner. The data will be monitored and quality assured, and the information will be managed following industry standards and is compliant with relevant legislation, through:

- Establishing a governance structure for the information held within the software, and that the data follows good practice guidance and has controls in place, to ensure the accuracy and timeliness of the data entered. Where any issues are identified, these are recorded, reported and dealt with immediately.
- Ensuring employees are aware that it is their responsibility to ensure the information held within FireWatch is accurate and correct, and that any changes needed should be reported to the People Section as soon as possible after realising an error, where this information cannot be changed themselves.
- Identifying and countering threats to information security and data protection.
- Controlling individual's access within the system, while ensuring they can undertake the role they are employed to do, whilst also limiting access to just the areas and information they need.

4. ASSOCIATED DOCUMENTS

- Equality Impact Assessment
- Legal Reference
  - Data Protection Act 2018, UK General Data Protection Regulation (UK GDPR)
  - Freedom of Information Act 2000
  - Copyright Designs and Patents Act 1988
  - Human Rights Act 1998
- National Guidance
  There is no specific National Guidance related to this policy.
- Data Protection Policy
- Records Management and Data Quality Policy.
- Disciplinary Policy

5. DATA MANAGEMENT

The Digital Services Manager is the designated Information Security Officer (the Corporate Assurance Section will deputise in their absence) and has day-to-day responsibility for Information Security, including:

- Monitoring and reporting on the state of Information Security.
- Ensuring that the Information Security Policy is implemented.
- Developing procedures to enhance information security arrangements.
- Ensuring compliance with relevant legislation.
- Ensuring that personnel are aware of their responsibilities and accountability for Information Security.
- Investigating reported breaches of Information Security; and,
- Monitoring for actual or potential Information breaches.

This policy, its implementation and systems will be subject to periodic review by both internal and external auditors.

6. SECURITY RESPONSIBILITIES

Management Responsibilities

Managers at all levels should ensure that:

- Employees are aware of their security responsibilities at induction and throughout their employment with the Service, including details on the Data Protection Act 2018, UK General Data Protection Regulation (UK GDPR) and Freedom of Information Act 2000, and that breaches in policy may lead to investigation under the Disciplinary Policy.
- Employees are given a suitable, and sufficient level of access to information needed to perform their role. Access needs over and above the default levels assigned by the HR Systems Auditor, shall be discussed with them to ascertain the areas not currently available to any individual.
- Employees are not able to gain unauthorised access to any information that would compromise data integrity or breach confidentiality. If a manager suspects a user may have more access than they require, they must contact the HR Systems Auditor immediately to investigate.
- Employees have access to read the Information Security Policy and associated Policy Delivery Guidance.

User Responsibilities

- Whilst access to Firewatch is linked to a user's own Microsoft login details, it is still the users responsibility not to give these details to anyone else or leave any electronic device unlocked. Doing so could mean that someone else has access, or could access, information held within FireWatch. This action would compromise both the security of the system and the information held within. Any breach of this nature would be dealt with via the Disciplinary Procedure.
- Each user is responsible for ensuring they do not amend anyone else's data, unless it is their responsibility to do so, as part of their job role, e.g. as a line manager.
- Each user is responsible, for ensuring that their own personal data held within FireWatch is accurate. Where data is found to be incorrect and the end user has the access to alter, then it is their right and responsibility to make any changes. Where incorrect information is found and the user does not have the ability to amend, they must contact the people section as soon as possible to correct. Failure to follow this procedure may lead to investigation under the Disciplinary Policy.
- Each user is personally responsible, for ensuring that no breaches of information security result from their actions. Any data breach should be reported to the data breach email address databreach@humbersidefire.gov.uk as detailed in the Personal Data

Breach Notification Policy Delivery Guidance.

- Each user is required to report any breach, or suspected breach of information security.
- Each user is responsible for ensuring that data entered as part of their job role is accurate and entered within a timely manner, ensuring that changes are made to maintain or improve data quality within the FireWatch system.
- Each user entering establishment data will always follow the defined and documented guidelines and process maps, ensuring consistency in entry of information. Anyone found not following the defined and documented instructions may be subject to investigation under the Disciplinary Policy.

HR Systems Auditor

The HR Systems Auditor will ensure that all team members who are responsible for the day-to-day management of people data, do so in accordance with the predefined agreed process maps. The HR Systems Auditor will also be the first point of contact regarding back-end system changes, user logins, security access and data quality management. Members of staff who have been trained, but fail to maintain data accuracy and timeliness, may be subject to performance management discussions.

The role responsibilities include:

- Granting and revoking user access and ensuing that access given is limited to the end users requirements
- Data quality auditing
- Data analysis and reporting
- Implementing and reviewing procedures to comply with data quality.
- Acting as the key contact with any third-party support.
- Undertake testing of software releases before release into the live environment.
- Work with end users to investigate and develop the software to assist with streamlining existing working processes.
- Understanding of the system and the underlying structure.
- Manages and creates users to access the Fire Watch system

7. RISK MANAGEMENT

Methodology

A register shall be maintained detailing any risks to the use / misuse of the FireWatch system, and any mitigating actions required to minimise identified potential issues.

This will also link to the business continuity arrangements that are in place for FireWatch, and detail mitigations around any loss of access to the system, and the responsibility of the end users in an event such as restrictions to access HR data, and alternative working processes to deal with such an event.

Reviews shall include:

- Identification of assets of the system.
- Evaluation of potential threats.
- Assessment of likelihood of threats occurring.
- Identification of practical cost-effective counter measures; and,
- Implementation programme for counter measures.

Systems are liable to independent reviews by internal and external auditors.

Reporting

Each system review will include a formal report back to Corporate Assurance containing any findings and further recommendations.

8. USER ACCESS CONTROL

Registering Users

Formal procedures shall be used to control access to the FireWatch system. An appropriate manager shall request access with an explanation of the role required to be undertaken by the user.

The HR system auditor shall then create the user account and assign the relevant security access groups to allow the user to be able to access the areas of the system to allow them to fulfil their role. This access is assigned to the associated post number of the role the individual will be undertaking. This means that if another individual is placed in that post number, they will automatically receive the necessary access required for that post.

Assigning security access to the post number ensures that the individual only has the access required for their role at that moment in time, and any people they manage. Assigning security to a user would be a more time-consuming task, as well as having the potential that a user keeps access they may no longer need if they moved job role.

If a manager deems that a particular role requires further access than is given when a post number is assigned, then as detailed in Section 7, Management Responsibilities, they will have to contact the HR systems auditor to discuss.

At user creation a PIN number is set to allow the user to authorise relevant actions. The user has the ability to change this PIN themselves, however if they have any problems, they should contact the HR Systems Auditor in the first instance.

User Credentials and Password Management

User credentials for the Firewatch system are created by the HR Systems Auditor and linked to the users Active Directory login. The Digital Services team can only access the Active Directory (AD) account access software to manage access to the organisations network.

This active directory login is required prior to the creation of the FireWatch user, as it is used to perform a single sign on login to the software, removing the need for the

end user to require a different login name and password.

All passwords are to be kept confidential. Passwords are the responsibility of the individual users; they must not be used by anyone else, even for a brief period.

Where there is a suspicion that the integrity of a password has been compromised, it is to be changed immediately. The giving of a password to another user to gain access to an information system will be investigated under the Disciplinary Policy. Individuals having a legitimate need to access systems will be given the appropriate password as required.

Employees Leaving or Changing Roles

Access to all systems is automatically revoked on termination of employment or change in role. It is the responsibility of line managers to request the removal or alteration of someone's access to both the system auditor and the Digital Solutions section.

Prior to an employee leaving, line managers working with HR shall ensure that:

- The employee is informed in writing that they continue to be bound by their confidentiality agreement.
- The Digital Solutions Section and the system auditor are informed to suspend user accounts.
- Where appropriate, employees in their 'notice period' are assigned to non-sensitive tasks or are appropriately monitored.

Data Backup

The FireWatch system is cloud hosted by LearnPro Group, and as such backup policies and procedures are in place and are the supplier's responsibility to ensure as a customer, we are protected from a data backup perspective. With this in mind, they manage the functionality of data backups.

It is still our own responsibility to ensure that we do not leave ourselves vulnerable to any other form of cyber-attack that could then lead to the FireWatch system being infiltrated.

Information held within the FireWatch database is encrypted where data is deemed to be of a sensitive nature, which is in line with data security principles.

Development, Test and Training Systems

Development and Test systems shall be separated from the live in use FireWatch version. As these systems contain archived or recovery data for testing purposes, they will be subject to the same security controls as the live system.

New versions of the FireWatch software and/or configuration changes shall be loaded onto the test system for checking of integrity and functionality prior to transfer to the live environment. All updates shall be supported by the system provider and all up to date documentation shall be provided where applicable.

9. DATA VALIDATION

At Data Input

Accuracy is the direct responsibility of the person entering, processing, or retrieving the data. The FireWatch system shall include enough validation processes at the data input stage to check in full or in part the acceptability of the data.

Any data error(s) found should be reported to the System Auditor in the first place, then corrected, and any relevant training or system correction shall take place to mitigate future repetition of the error(s) found. Users should not just ignore any incorrect information they come across as part of their daily tasks but work proactively in ensuring that the information within FireWatch is accurate at all times.

Any loss or corruption of data shall be reported to the HR System Auditor immediately.

Internal Validation

All systems shall incorporate internal validation processes and audit trails to detect and record problems with processing/data integrity.

Data protection legislation places a requirement on the Service to ensure any personal data they collect, and process, is accurate and kept up to date. Further guidance is provided in the Data Protection Policy and the Records Management and Data Quality Policies.

10. SOFTWARE USAGE, PROTECTION AND PRIVACY

Users will be given access to the FireWatch system to allow them to undertake tasks that are relevant to themselves, such as booking leave, sickness absence, and keeping their own personal information up to date.

As well as the above, extra access will be given to those members of staff who manage other people as part of their role and this additional functionality will be linked to the post number and role within FireWatch. This is another example where correct processes and procedures must be followed to ensure data quality and security is maintained.

Information Protection

All personal characteristic data is encrypted within the FireWatch database and cannot be viewed from the database directly. The data can only be viewed using the FireWatch front end web client or App. Each individual with access to FireWatch will be able to see only their own personal data. An additional number of staff elsewhere within HFRS will also have access but only where it is relevant as part of their role.

11. DISASTER RECOVERY PLANNING

Need for Effective Plans

The Service shall plan for business continuity in the event that the FireWatch system became unavailable and will have scalable arrangements in place to cater for a wide range of situations. The development of new systems shall incorporate resilience by design and have in place adequate arrangements proportionate to the risk associated with permanent loss of the system.

Copies of plans shall be stored in other on-line and local locations so that they can be instigated without having to rely on only one method of retrieval.

The disaster recovery plan will include:

- Fallback procedures describing the actions to be taken to provide contingency devices.
- Recovery time objectives.
- Resumption procedures describing the actions to be taken to return to full normal service.
- Testing procedures describing how the disaster recovery plan will be assessed.

12. LEGISLATIVE FRAMEWORK

In discharging its duties, the Service recognises the following legislation that impact on this FireWatch Policy:

Data Protection Act 2018

Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR)

The purpose of the legislation is to protect the rights and freedoms of individuals about whom data is obtained, stored, processed, or supplied. This applies to both computerised and paper records.

The Service shall comply with the registration requirements of the Data Protection Act 2018 and the UK General Data Protection Regulations (UK GDPR). They require that appropriate security measures will be taken against unauthorised access to, or alteration, disclosure, or destruction of personal data and against accidental loss or destruction of personal data.

The Act is based on seven principles stating that data must be:

- Lawfully, fairly, and transparently processed.
- Collected for specific, explicit, and legitimate purposes.
- Adequate, relevant, and limited to what is necessary for processing.
- Accurate and kept up to date.
- Not kept longer than necessary
- Processed in a manner that ensures appropriate security is an overarching principle that the service is accountable and must be able to demonstrate compliance with the other principles.

Computer Misuse Act 1990

This Act states that it is a criminal offence to attempt to gain access to computer information for which you have no authorisation. If it is suspected that any unauthorised access is made to a computer system, this shall be investigated under the Disciplinary Policy and may be reported to the Police.

Human Rights Act 1998

Under Article 8 of the European Convention on Human Rights, personal data is part of an individuals' 'private life' and as such they have the right to have such information treated in the strictest confidence.

Freedom of Information Act 2000

The Freedom of Information Act provides a right to request access to information held by the Public Authorities and, subject to certain exemptions, the Service is required to disclosure whether it holds the information requested and release that information within twenty working days.

For further guidance or information relating to this document please contact Head of Human Resources