HUMBERSIDE FIRE AND RESCUE SERVICE

# Service Improvement

## Information Security Policy

| | |
|---|---|
| **Owner** | **Executive Director of Corporate Services** |
| **Responsible Person** | **Head of ICT** |
| **Date Written** | **February 2010** |
| **Date of last review** | **March 2023** |
| **Date of next review** | **March 2024** |
| **EIA Completed** | **23 August 2021** |

What we must do well

How we support our communities

We value and support the people we employ

We efficiently manage the Service

# CONTENTS

## 1. INTRODUCTION

The confidentiality, integrity and availability of information produced, handled, and stored by the Service is paramount to ensure the safety of the local communities, protect the safety of its own personnel, and demonstrate sound governance, including compliance with legislative requirements.

The Information Security Policy applies to all employees and others not employed by the Service but engaged to work with or who have access to Service information. It also applies to all locations where Service information is accessed or stored (including non-Service locations).

The policy applies to all information including manual, electronic and verbal. The level of security applied to information will balance the cost against risk.

### 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 which has been adopted by HFRS, will be reflected in this Policy.

## 2. EQUALITY 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 nor 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

To make sure the Service’s information security is effective, follows industry standards and is compliant with relevant legislation, through:

- Establishing a management structure for information security that follows good practice guidance and has controls in place balancing cost and risk. Whereany question arises over the primacy of policies, the requirements for Information Security shall take precedence.
- Ensuring employees are aware of security risks and their responsibilities to minimise threats.

- Identifying and countering possible threats to the information security and standards.
- Controlling individual's access to systems they require for their role.

## 4. ASSOCIATED DOCUMENTS

- Equality Impact Analysis
- Legal References
    - Data Protection Act 2018, UK General Data Protection Regulation (UK GDPR)
    - Freedom of Information Act 2000
    - Copyright Designs and Patents Act 1988
    - Computer Misuse Act 1990
    - 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. POLICY STATEMENT

Information security is a shared responsibility. Confidentiality, integrity, and availability of information can be compromised at any point in the information flow.

The Service is committed to ensuring all the information it controls will be managed securely throughout the life cycle of the information, from creation, to disposal, by utilising a combination of manual processes and technical solutions:

- Maintaining the integrity and availability of ICT assets.
- Maintaining confidence in data accuracy for use in decision making.
- Compliance with the law on licensed products and minimise the risk of cyber security breaches.
- Ensuring the ability to restore computer facilities to maintain essential activities following a major failure or disaster.

## 6. SECURITY MANAGEMENT

The ICT 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.

## 7. SECURITY RESPONSIBILITIES

### Management Responsibilities

Managers at all levels should ensure that:

- Employees will only use HFRS' supplied equipment to connect to the HFRS network infrastructure and software systems. Anyone connecting not using a HFRS supplied device, may be subject to investigation under the Disciplinary Policy.
- Employees are aware in 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.
- Employees are not able to gain unauthorised access to any information that would compromise data integrity or breach confidentiality.
- Employees using computer systems and storage media are adequately trained in their use.
- Documentation is maintained relating to all critical job functions to ensure it can be accessed to enable continuity in the event of individual unavailability.
- Employees are aware of the Constitution rules on potential personal conflicts of interest.
- Employees, contractors, and visitors sign confidentiality (non-disclosure) undertakings before commencing work.
- The relevant System Managers and the ICT Section are advised immediately about staff changes affecting computer access (e.g.,

job function changes/leaving department or organisation) so that accounts can be deactivated or amended.

- Employees have access to read the Information Security Policy and associated Policy Delivery Guidance.

## User Responsibilities

- Employees will only use HFRS supplied equipment to connect to the HFRS network infrastructure and software systems. Anyone connecting not using a HFRS supplied device, may be subject to investigation under the Disciplinary Policy.
- Each user is personally responsible, for ensuring that no breaches of information security result from their actions.
- Each user is required to report any breach, or suspected breach of information security.
- Each user must ensure that any equipment provided by HFRS is used only for its original intentional distribution purpose and will not be used for personal or non-HFRS related business or transactions. This includes items such as mobile phones, laptops, desktop computers etc.

## Protective Security Group

The Protective Security Group (PSG) is made up of representatives from across the Service with relevant roles and job functions. It shall have the following objectives:

- Ensure that security activities are carried out in accordance with the InformationSecurity Policy and associated Policy Delivery Guidance and relevant Standards including ISO 27001.
- Identify how to handle non-compliances with the Information Security Policy and associated Policy Delivery Guidance.
- Recommend and approve processes for information security, e.g., information classification, access control, data retention and disposal.
- Identify where exposure to different threat levels could impact upon the security environment.
- Assess the adequacy of the implementation of information security controls throughout HFRS.
- Support the implementation of information security awareness training.
- Evaluate information received from the monitoring and reviewing of information security incidents and recommend appropriate actions in response to identified incidents.
- Own the Risk Treatment Plan (RTP) and monitor the treatment of identified risks.
- Recommend for approval by SLT, the internal audit programme for

theInformation Security Management System (ISMS); and,

- Act as Champions for information security throughout HFRS and activelypromote good practice.

## System Manager

Each system shall have a designated System Manager, with responsibility for the day-to-day administration of that system, whether paper or IT based. The role should include:

- Granting and revoking user rights and ensuing that only authorised individuals have access to the system.
- Ensuring adequate password management is in place (e.g., complexity, length, structure, history).
- Implementing and reviewing procedures to comply with the information security policy.
- Ensuring there are adequate support arrangements to cover for absence, busyperiods, etc.
- Acting as the key contact with any third-party support.
- Undertake testing of software releases before release into the live environment.
- Undertaking security risk assessments on the system; and,
- Understanding of the system and the underlying structure.

## Information Asset Owner

Each Head of Function will assume the role of Information Asset Owner for their area of the business and will be responsible for:

- Authorising requests to access information (e.g., shared network areas,personal record files, fire safety records, etc.).
- Assessing the adequacy of controls that are in place for securing protectively marked information contained within systems for which they are responsible.
- Championing information security within the functional area.
- Locating information requested under the Data Protection Act 2018, UK General Data Protection Regulation (UK GDPR) Freedom of Information Act 2000, and similar legislation.
- Regular review of their information assets recorded in the Service's Information Asset Register.
- Approving the disposal and destruction of records in accordance with documented retention periods.

### Head of Human Resources

The Head of Human Resources shall ensure that:

- all individuals are adequately screened for suitability prior to initial appointmentand on change of role.
- induction programmes include Information Security as a theme.
- contracts for employees, and anyone who may be contracted to provide services, include confidentiality (non-disclosure) agreements together with a clause reserving the copyright on all items created in the course of employment.
- Terms of Conditions of employment reflect the current Information Security Policy and associated Policy Delivery Guidance.

## 8. RISK MANAGEMENT

### Methodology

A register shall be maintained detailing each information system, associated assets, storage location, Systems Manager, and protection requirements. This shall be updated as systems change, reviewed regularly and always after a major security incident. An assessment of all risks shall be made for each information system to ensure that it is secured appropriately. Systems shall be reviewed periodically based on a risk profile.

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.

Projects that introduce new information systems shall be subject to the same security considerations as live systems and shall be subject to Risk Assessment for adequacy of security controls.

### Reporting

Each system review will include a formal report to the Protective Security Group containing findings and recommendations.

## 9. USER ACCESS CONTROL

## Registering Users

Formal procedures shall be used to control access to IT systems. An appropriate manager at Group Manager level/Grade 13 or above shall be required to support each application request and review their support at regular intervals, including the level of access rights provided.

## User Credentials and Password Management

User credentials are created and held within the Active Directory (AD) software that is used by the ICT team to manage access to the organisations network.

The ICT team are the only people who have access to the AD software, and this allows strict controls to the creation, amendments, and access of all HFRS staff and suppliers, that require login credentials for the organisations network.
User credentials for other systems are allocated to a restricted number of people who require access to fulfil their job role. Access is controlled by the system administrator of each applicable piece of software.

The complexity requirement for passwords shall vary depending on the level of protection needed for the information.

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.

Systems shall force password changes at regular intervals and a history will be maintained to prevent password reuse within a reasonable period. Sessions shall time-out to a screen saver or terminate the session after a reasonable period of inactivity; users will be required to re-enter their password to reactivate their session.

## 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 de-registering of users.

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 ICT section and other System Managers are informed to suspend user accounts.

- Receptionists and others responsible for controlling access to premises are informed of the termination and are instructed not to admit them without a visitor’s pass.
- Where appropriate, employees in their ‘notice period’ are assigned to non-sensitive tasks or are appropriately monitored.
- That all files that continue to be of interest to the activity of the service are transferred to another employee. Where the circumstances of leaving make it likely that an individual might inappropriately delete or destroy information, then access rights should be restricted to protect the information and equipment.
- Service property is returned.

The timing of these requirements will depend upon the reason for termination and the relationship with the employee. Where the termination is mutually amicable, the withdrawal of such things as passwords and keys may be left to the last day of work, if this differs from the last day of employment (i.e., because of taking leave and time owing, etc.).

Managers should bear in mind that once an employee has left, it is virtually impossible to enforce security disciplines, even via legal processes. Evidence from elsewhere shows that many cases of unauthorised access to information can be traced back to information given out by former employees.

System Managers shall deactivate or delete all user access codes relating to individuals leaving the Service.

Employees leaving the Service or changing role are not permitted to buy or transfer ownership of computer equipment, telephones (including telephone number) or any other resources assigned to them in the course of their employment.

### Employees with Dual Access Accounts

Many employees can log onto computer systems with more than one username. These include Watch Managers and Crew Managers, who may require access to a Station area as well as access to a personal account. Logging on as a Station user will give access to general (not protectively marked) information but logging on as a specific named user may give access to information of a more sensitive nature where protective marking may apply. Under these circumstances, managers must ensure that information of a sensitive nature is not accessible from the general area, and must therefore ensure that whenever producing, handling, or storing such information that this is strictly within the specifically named access area only.

### Action under Disciplinary Policy

Managers, in conjunction with investigating officers, shall consider whether it is appropriate to suspend, down-grade system privileges, or prohibit access to secure areas, for employees who are subject of investigation under the Disciplinary Policy, and where there is a serious risk to maintaining the principles set out in the Information Security Policy and associated Policy Delivery Guidance. This also includes situations where there is a risk that evidence may be lost by allowing access to continue at the same level. These measures shall remain in place until such time as the risk diminishes.

### Visitors and Contractors

Where temporary user credentials need to be issued to allow access to computer systems, these shall be disabled when the visitor has left. Visitors will only be given access to the system(s) required to complete the work they have been contracted to undertake.

## 10. HOUSEKEEPING

### ICT Equipment End of Life / Disposal

1. Storage media will be physically removed from any ICT equipment and after a period of 3 months, will be given to a licensed third-party contractor for safe disposal. This contractor will provide certificates verifying that storage media has been safely disposed. The certificates will include the asset numbers of the originating hardware and the serial numbers of the storage media. (Where storage media cannot be removed, the device will be made inactive or disposed of by ICT staff in line with WEEE guidance) The remaining components will be disposed of in line with WEEE guidelines.

2. Mobile phones - it is the user’s responsibility to transfer any contact details to another device before surrendering for disposal. Mobile phone, SIMS and memory cards will be physically destroyed and will not be recoverable. The ICT department is not liable for the retrieval of data recorded on any mobile phone, SIM, or memory card.

Below sets out the procedure when disposing of ICT Equipment:

- Update CMDB using the Blue Sticker/Asset number to confirm its disposal
- Update Active Directory to show the equipment has been taken from the ICT Infrastructure
- Place in the Disposal Cage (located SHQ on the ground floor)
- Update the disposal sheet with the Blue Sticker/Asset number

Once the cage has been collected, we will be given an electronic list of the Asset Numbers or Serial Numbers if they were not labelled.

### Data Backup

Data should be held on networked file servers where possible, to ensure that it is captured by routine backup processes. Where information is held on a PC hard drive or PC desktop (their profile), the user is responsible for backups and ensuring the security of these backups. Where portable or removable media is used for backup purposes or for holding live versions of files, this shall be subject to the same security controls as all other information.

Data shall be protected by clearly defined and controlled backup procedures which will generate data for archiving and contingency recovery purposes. Backup copies of data shall be accurate and sufficient to restore to an agreed point.

The ICT Section and System Managers shall produce written backup instructions for each system under their management. The backup copies shall be clearly labelled and held in an off-site, or off-line secure location. Procedures shall be in place to recover to a useable point should a restore be necessary. These shall be periodically tested. A cyclical system of backups will be used.

Archived data is defined as data that is no longer in current use, but may be required in future, for example, for legal or audit purposes. Recovery data is defined as current data that is needed to run the organisation that is securely stored for use under business continuity that can be recovered within a reasonable timeframe. Recovery data shall be graded in order of significance in terms of criticality to restore a normal service.

Archived and Recovery data shall be accorded the same security as live data and shall be held separately. Archive and Recovery data can only be used with the formal permission of the System Manager, or as defined in the Business Recovery Plan. Retention of Archived and Recovery data shall be proportionate to business requirements.

Where live data is corrupted, all relevant software, hardware and communications equipment shall be checked by the System Owner and ICT Section before using the backup data.

## Development, Test and Training Systems

Development, Test and Training systems shall be separated from live systems. When they contain archived or recovery data for testing purposes, this shall be subject to the same security controls as live systems.

New versions of 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. Appropriate change control documentation shall be signed by the System Manager before releasing new versions of software to the live environment. All updates shall be supported by the system provider and all up to date documentation shall be provided.

## Controlled Stationery and Asset Tags (e.g., payment stationery, official orders, etc.)

Formal procedures shall be used to control and account for the use of such items. Each item shall include some form of unique identifier to assist control management.

## 11. DATA VALIDATION

### At Data Input

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

Systems shall be required to report all errors together with a helpful reason for the rejection to facilitate correction. Error correction shall be done at the source of input as soon as it is detected.

Any loss or corruption of data shall be reported to the relevant System Manager 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 Policy.

## 12. SOFTWARE USAGE, PROTECTION and PRIVACY

Users have full access and use of the Microsoft O365 suite of products, including Teams, OneDrive, Outlook etc, that are related to their roles and requirements. However, it is the individual’s responsibility in the use of these products and must adhere to other people’s privacy and data protection. This means that the recording of Teams meetings is prohibited without the explicit consent of all those attending. If one individual objects, then the meeting must not be recorded.

Any personal data saved on HFRS hardware, or on HFRS licenced OneDrive areas, becomes the property of HFRS, and as such will be included in any subject access requests searches, or Disciplinary Investigations.

The use of WhatsApp within the service is for work and Business Continuity arrangements only and should not be used for any other purpose.

### Licensed Software

The ICT Section shall be responsible for ensuring that all approved software is properly licensed. The ICT Section shall also maintain a register of software assets and is responsible for the security of licence agreement's Software Standards

The ICT Section shall be responsible for maintaining a list of software and approved versions. All software installations shall be carried out by the ICT Section. Only authorised software shall be loaded onto a computer. Unauthorised software and associated files found on computer equipment will be removed immediately by the ICT Section and may be investigated under the Disciplinary Policy.

### Virus Control

Anti-virus software is installed on all appropriate computer equipment, and this will be automatically updated with virus definition files. Inbound e-mail messages shall be subject to anti-virus, anti-spam, and other malicious code scanning. Infected messages will be quarantined and deleted. Where messages are quarantined, recipients will receive a message advising them this has occurred.

## 13. DISASTER RECOVERY PLANNING

### Need for Effective Plans

The Service shall plan for business continuity and 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 at off-site locations so that it can be instigated without having to access Service premises.

### Planning Process

The main elements of this process include:

- Identification of critical computer systems.
- Identification and prioritisation of key users/user areas.
- Agreement with users to identify disaster scenarios and what levels of disasterrecovery are required.
- Identification of areas of greatest vulnerability based on risk assessment.
- Mitigation of risks by developing resilience.
- Developing, documenting, and testing disaster recovery plans, identifying tasks, agreeing responsibilities, and defining priorities.

### Planning Framework

Disaster recovery plans will cater for various levels of incident including:

- Loss of key user area within a building
- Loss of a key building

- Loss of key part of computer network
- Loss of processing power
- Loss of key personnel

Disaster recovery plans will include:

- Emergency procedures covering immediate actions to be taken in response toan incident (e.g., alerting disaster recovery personnel).
- Fallback procedures describing the actions to be taken to provide contingency devices.
- Recovery time objectives and critical systems to be restored first.
- Resumption procedures describing the actions to be taken to return to full normal service.
- Testing procedures describing how the disaster recovery plan will be tested.

## 14. LEGISLATIVE FRAMEWORK

In discharging its duties, the Service recognises the following legislation that impact on its Information Security 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.

Copyright Designs and Patents Act 1988

### Copyright, Designs and Patents Act 1988

The Act states that it is illegal to copy and use software without the copyright owners' consent or the appropriate licence to prove the software was legally acquired. System Managers shall be responsible for ensuring that all their installations are covered by an appropriate licence.

Any infringement or breach of software copyright may result in personal litigation by the software author or distributor and may be investigated under the Disciplinary Policy.

### 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 20 working days.

**For further guidance or information relating to this document please contact ICT**