HUMBERSIDE FIRE AND RESCUE SERVICE

# Service Improvement

## Cyber Security Policy

| | |
|---|---|
| **Owner** | **Executive Director of Service Improvement** |
| **Responsible Person** | **Head of ICT** |
| **Date Written** | **December 2022** |
| **Date of Last Review** | **December 2022** |
| **Date of next review** | **December 2024** |
| **EIA Completed** | **December 2022** |

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

Humberside Fire and Rescue Service (HFRS) uses, stores, collects, and shares a wide range of information in delivering its services to the community, including members of the public, other agencies, and emergency services. It also holds personal data for all employed staff members within its HR software system.

There are a wide range of options and benefits to electronic storage and digital solutions, as well as multiple ways to achieve this. However, the first option for any solution and the information it holds, is to ensure that the systems and processes in place are regularly assessed, improved, monitored, and acted upon to maintain data integrity and security, as appropriate.

Cyber security should be one of the top priorities for organisations that hold, process, and share data and information, and therefore a robust set of policies, procedures, and mitigations need to be in place to support this. Cyber security breaches are now commonplace in all sizes of organisations, and these range from small data breaches to full blown attacks that disable an organisation's complete infrastructure, along with its access to some or all of the data and information it holds.

The information that HFRS holds, processes, maintains, and shares, is an important asset that, like other important business assets, needs to be suitably protected. In order to build organisational and public confidence, and to ensure that HFRS complies with relevant statutory legislation, it is vital that HFRS maintains the highest standards of information security and has policies to support and maintain these standards.

This policy sets out the overall objective and principles for cyber security at HFRS and specifies the management arrangements and key responsibilities. This policy will be supported by other detailed documents covering more specific aspects of information security and associated management and controls. (Section 4. Associated Documents)

### Core Code of Ethics

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 & 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

The aim and objectives of this Cyber Security policy and its supporting policies is to ensure the highest standards of cyber security are always maintained across HFRS so that:

a) All users are aware of the need for confidentiality in regarding usernames and passwords, the systems they access, and the things they need to be aware of to reduce the risk of instigating or contributing to a cyber incident breach.

b) Business damage and interruption caused by cyber security incidents are minimised, and full recovery planning regimes are reviewed, tested, revised, and amended as appropriate.

c) All associated polices, and procedures will be followed to mitigate as far as is possible, the chance of being successfully targeted by cyber criminals.

d) All legislative and regulatory requirements are met.

## 4. ASSOCIATED DOCUMENTS

- Equality Impact Analysis (temporary link for the purposes of consultation)
- Data Protection Policy
- Information Classification Policy
- Information Security Policy
- Internet Email and Instant Messaging Policy
- Personal Data Breach Notification Policy Delivery Guidance
- Records Management and Data Quality Policy
- Information and Security Risk Guidance (consultation pending)
- Legal References
    - Prevent Duty, Counterterrorism and Security Act 2015.
    - The Data Protection Act 2018
    - General Data Protection Regulation (GDPR)
- National Guidance Reference
  There is no specific National Guidance relevant to this policy.

## 5. SCOPE

This policy applies to anyone who has a username, email account, or any other electronic access to any HFRS network, software system, or digital equipment.

The policy applies automatically to all HFRS staff, Fire Authority Members, Directorates, Sections, Agency Partners, contractual third parties and all other organisations, and people who interact with HFRS. Where access is to be granted to any third party (e.g., contractors, service providers, voluntary agencies, and partners) compliance with this policy must be agreed to and documented.

## 6. LEGAL AND REGULATORY OBLIGATIONS

HFRS depends on the confidentiality, integrity and availability of its information and digital systems to such an extent that any cyber security breach could have a detrimental impact on HFRS's ability to deliver a wide range of statutory services.

HFRS should also consider whether digital equipment available to the general public should use filtering solutions that limit access to terrorist and extremist material under the Prevent Duty, brought in as part of the Counterterrorism and Security Act 2015.

In addition, HFRS has obligations to ensure robust cyber security is in place if it is to use or share information electronically with partner agencies under information sharing arrangements.

## 7. POLICY RESPONSIBILITIES

### Strategic Approach and Principles

This policy evidence's the commitment of senior management to achieve and maintain a high standard of cyber security throughout HFRS. The strategic approach to cyber security is based on:

- The application of recognised sources of cyber security management standards and guidance as detailed by the National Cyber Security Centre (NCSC) ten steps to reduce cyber risk and other Home Office departments.
- Attain Cyber Security Plus Accreditation and fully implement all associated policies and procedures as required.
- Six monthly testing of HFRS's ICT Cyber Business Continuity Recovery Plan.
- The continuing availability of specialist cyber security advice to support the ongoing development and maintenance of cyber security levels at HFRS.
- That cyber security remains on the Corporate Risk Register and the Strategic Leadership Team (SLT) are kept aware of any changes in specific Public Sector, or Emergency Service Threat levels.

### Approach to Information Security and Risk Management

The Information Security Policy sets out HFRS's approach to information security management and the key roles and responsibilities under that policy. Reference to this policy can be found in Section 4 Associated Documents.

### Key Elements of Cyber Security Policy Management

This policy will be supported by more detailed procedures, standards, guidance, and training that aligns to recognised sources of security management good practice, such as appropriate use of HFRS assets, information retention period standards etc.

### Awareness of the Cyber Security Policy and Procedures

The Cyber Security Policy, and associated procedures, will underpin mandatory corporate training, and periodic refresher training for all HFRS staff. The training will be supported by further information available on the HFRS SharePoint site. Users' competency and training completion is monitored and reported on, and any users not undertaking the necessary training relating to cyber security and other related subject areas, will be dealt with in accordance with HFRS HR policies.

## 8. ROLES AND RESPONSIBILITIES

It is important that a clear distinction is drawn between the responsibilities for all users, managers, and the ICT Section. Cyber security must not be seen as the sole responsibility of the ICT Section. The majority of cyber security breaches occur at the end user point of contact, and consequently, requires the attention of all staff, in order to adequately protect HFRS and its network infrastructure, systems, and information it holds from any potential external threats.

### ALL USERS

There are a number of other key issues and practices that work hand in hand with good cyber security, and all HFRS users must be aware of and comply with those relevant HFRS policies. These are listed in Section 4. Associated Documents.

### Home and Mobile Working

Digital security access is centred on each authorised user having a unique user ID and a strong password, that is kept secret and known only to them. User ID and passwords must not be shared or used by anyone other than the authorised user. Contraventions of this requirement will be investigated under the Disciplinary Policy. Mandatory cyber security and other recommended training to understand the risks involved will be provided and expected to be undertaken.

### User Education and Awareness

### Data Protection

The Data Protection Act 2018 in conjunction with the General Data Protection Regulation (GDPR) is the key legislation affecting the use of personal data. Illegal or accidental disclosure of personal information, such as a cyber-attack could lead to HFRS, or the individual responsible, being prosecuted and/or heavily penalised. All

employees are expected to understand and comply with this Act. Any suspected Data Breaches should follow the procedures as explained in the Personal Data Breach Notification Policy Delivery Guidance.

**Information Handing**

Information security and handling procedures are designed to protect HFRS from identified business impacts in the event of the loss of confidentiality, integrity, or availability of information such as in a cyber-attack.

**Work Environment**

Clear desk policy implementation, ensuring digital equipment is secure when not in use, as well as undertaking mandatory and recommended information governance training, and be aware of the HFRS's Information Governance Framework and associated policies.

**Incident Management**

Users must be able to identify potential cyber security risks, or attempted attacks and act appropriately when they occur, by following procedures set out in this Policy, and as detailed in additional e-Learning modules.

**Cyber Risk Management Regime**

Communicate any potential error messages, strange electronic communication, or anything that looks out of the ordinary, immediately to the ICT Service Desk. Even if this turns out to be a non-incident, it is vital that all of these types of potential risks are investigated to ensure that the cyber security levels are maintained and adapted to mitigate similar future incidents occurring.

**Managing User Privileges**

Employees, agency staff, contractors and third parties, will be given individual accounts and access to information that will be limited, based on the need and requirements of the role, and tasks being undertaken. Full details of User Responsibilities can be found in Section 7 of the Information Security Policy.

**Removable Media Controls**

Removable media is not to be used or connected to any device unless permission has been given by the appropriate line manager. The device must be presented to the ICT Section, where it will be scanned for malware before a decision of connecting the device to the corporate network is even considered. Anyone found trying to connect and access removable media without following the above procedure, will be subject to HR conduct and performance procedures.

**Monitoring**

Report any unusual activity to the ICT Service Desk.

## MANAGERS

Managers are responsible for ensuring that they and the staff for whom they are responsible:

- Are aware of, and comply with, their responsibilities under the headings detailed above in ALL USERS.
- Undertake all identified mandatory Cyber Security and Information Governance training. In addition, they have responsibilities for the following.

### Home and Mobile Working

Assess the risks to all types of home and mobile working and ensure employees have received suitable training and guidance.

### User Education and Awareness

Ensure that staff undertake and successfully complete all appropriate cyber security training as part of the employee PDR's and maintain user awareness of cyber risks.

### Incident Management

Ensure plans are in place to recover from any disasters and maintain business continuity plans and documentation, and respond to any actual or potential cyber incident, in accordance with the HFRS's Business Continuity and Emergency Preparedness guidance documents.

### Cyber Risk Management Regime

Managers will ensure that the ICT Section are informed of any identified cyber risks that are reported to them, or that they find themselves. These will be recorded on the ICT Cyber Risk Register and will ensure that assurances are put in place to mitigate such risks. Controls will be in place to enable the tracking of digital equipment used off site, and it is the managers responsibility to ensure that all assets are collected at employment termination and returned to the ICT Section.

### Managing User Privileges

Managers will ensure that user access will be granted at a level that allows them to perform their day-to-day user activities and prevents access to any sensitive information not required for the purpose of undertaking their duties.

Managers will ensure members of staff, contractors, and third-party access to information systems does not exceed the needs of the role on a 'need to know' basis. They will ensure that their use of digital equipment and systems is appropriate, and that starter, leaver and amendment changes are properly processed and authorised.

Managers will ensure that where necessary, security and confidentiality agreements are in place for non-HFRS staff (including for example, contractors, students,

volunteers, partner agency workers) where personal or confidential information may be accessed.

### Removable Media Controls

Managers will ensure that all staff are aware that removable media is not permitted unless prior approval is granted to such devices. This is to reduce, as far as possible, the chances of the introduction of cyber related threats onto the HFRS ICT infrastructure and all associated and connected systems and devices. Managers will also follow the guidance around removable media as detailed in Removable Media Controls under ALL USERS above.

### Monitoring

Managers will ensure that staff report any unusual activity to the ICT Service Desk and ensure compliance with HFRS's Information and Cyber Security and Governance policies is maintained.

### ICT SECTION

The ICT Section are responsible for documenting and maintaining the wide range of technical standards required to enable the Cyber Security Policy, in line with best practice and Government guidelines.

These include standards for the following:

Network Security and Monitoring, Secure Configuration, Malware Prevention, Removable Media Controls, User Access/Permission controls, Change Control, Backup and Restoration, Threat Vulnerability Management etc.

ICT staff will also be responsible for ensuring the following is adhered to, monitored, and maintained:

- Full change control procedures will be followed before any security patches or changes are made to Hardware, Network, or Software Systems. Documentation, detailing the implications of any changes, as well as full rollback procedures will be required, along with authorisation of those changes. This includes live elements like, servers, firewalls, switches, windows updates.
- Security risk status will be reviewed daily, and any mitigations will be dealt with within 14 days. This will work in conjunction with the patch Tuesday release schedule and will be planned and implemented according to the cyber update procedures.
- Backups will be implemented, monitored, and maintained as appropriate, including bi-annual restoration testing as a minimum for key hardware and software.
- Business continuity plans will be maintained and updated as required.

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