HUMBERSIDE FIRE AND RESCUE SERVICE

# Service Improvement

## Information Classification Policy

| | |
|---|---|
| **Owner** | **Executive Director of Corporate Services** |
| **Responsible Person** | **Head of Corporate Assurance** |
| **Date Written** | **October 2018** |
| **Date of Last Review** | **January 2024** |
| **Date of next review** | **January 2025** |
| **EIA Completed** | **May 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

This Policy forms part of the Service's Information Security Management System (ISMS). In conjunction with the Information Classification Scheme (Appendix A) it defines a standard method for the protective marking of information assets to ensure they are correctly managed and safeguarded throughout their lifecycle, including creation, storage, use (including transmission) archive and destruction.

### 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, DIVERSITY & 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 purpose of the Policy is to ensure the Service is able to effectively manage all information assets through their life cycle from creation to disposal. This will be achieved by:

- Aligning to the principles of the Government Security Classifications 2023.
- Staff assigning the correct information classification to assets created.
- All staff being mindful of the information classification assigned to documents and handling them in accordance with their respective classification.
- Maintaining compliance with other related legislation.

## 4. ASSOCIATED DOCUMENTS

- Equality Impact Assessment
- **Legal References**
  - Data Protection Act 2018;
  - UK GDPR

  - Freedom of Information Act 2000
  - Local Government Act 1972,
  - Children Act 2004,
  - Access to Health Records 1990.
  - Official Secrets Act 1989
  - Government Security Classifications (June 2023)

- **National Guidance**
  Control Measure – Data and information management

- Records Management and Data Quality Policy
- Disposal and Destruction of Records Policy Delivery Guidance
- Information Security Policy

## 5. DEFINITIONS

An information asset is defined as a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles. In the context of Information Classification that includes:

- Reports
- Letters and Correspondence
- E-mail and other electronic messages
- Plans and Diagrams
- Research
- Surveys and Questionnaires
- Conversations and other verbal communication
- Information Systems

## 6. CLASSIFICATION

All information assets shall be placed into one of four classifications. The classification assigned to an asset will determine how that asset should be managed, throughout its lifecycle. Classification should be proportionate to the sensitivity of the information and the impact of compromise and the capability and intent of threat actors likely to seek that information.

The classifications are, in increasing sensitivity:

1. Not Protectively Marked
2. Official
3. Secret
4. Top Secret

The HFRS Information Classification Scheme is underpinned by the principle that information is Not Protectively Marked, ie. it is suitable for public release, unless there is a legitimate reason for an increased (more restrictive) classification[1].
Higher classification shall be used only when assets:

- Fall into the higher categories set out in Appendix A.
- Are provided by a third party and are marked at a higher level.
- Relate to individuals and are covered by data protection legislation (Data Protection Act 2018 and UK GDPR).
- Would be exempt from disclosure under the Freedom of Information Act 2000.
- Are subject to other provisions in law, e.g. Local Government Act 1972, Children Act 2004, Access to Health Records 1990, etc.

Appendix A provides more details on the types of documents and information assets which are likely to attract a particular classification.

Where any doubt exists, a higher classification shall be applied until such time as clarity is received.

All protectively marked assets shall clearly show their classification, although it should not be assumed that an unmarked asset is Not Protectively Marked. For documents generated by the Service, this protective marking shall be included in the document footer on each page. Other documents, including those received by the Service, shall be marked by way of a stamp, handwritten note, etc. on the top of the asset. Verbal communication is covered by this guidance and all parties must be made aware if the subject matter is covered by one of the classifications.

The Service recognises that on occasions, operational requirements, in order to either save life or reduce the risk of serious injury, will require this guidance to be contravened e.g. adopting different handling procedures. This will be permitted as an exception, if a risk assessment has been conducted concerning the release of those information assets where the consequences of not releasing the material outweigh those of compliance, and then the risk may be considered necessary. Each individual breach of policy will be separately addressed.

## 7. CREATION AND MARKING OF ASSETS

Authors shall be responsible for classifying assets they create. As well as assessing the sensitivity of the information and the impact of compromise, authors must also

[1] This approach varies from the Government Security Classification (Jun 2023) which deems all information should be classified Offical, but enables publication of some by classifying as ‘Official – For Public Release’.

consider any genuine need-to-know or need-to-share. Further guidance on assigning classification scan be found at Appendix A.

It is essential that over-classification of assets is avoided as this may result in the intended target audience being unable to access the asset, or that it cannot be transmitted.

All Service forms shall not be Protectively Marked until they are completed. At this point they shall be assigned a classification relevant to their sensitivity. This classification shall be determined by the Head of Function that holds the completed forms.

Recipients of information assets from third parties shall be responsible for classifying that asset and this shall not normally be lower than any marking attached by the originator.

Routine marking of 'legacy documents' shall not be carried out, except in relation to assets extracted for movement/transfer or, where the asset becomes 'live'. Hard copy legacy assets shall be marked front and rear, rather than on every page, if securely bound together.

Digital Services have deployed a software solution across the network which is used to apply protective marking to e-mail messages. The classifications available in this system have been tailored to the Service's information classification scheme. Currently this system only applies the classification to the e-mail message, it does not automatically apply the classification to any attachments. Therefore, staff are responsible for ensuring any document attached to an e-mail shows a protective classification appropriate to the content and that no lesser classification is assigned to the e-mail message.

Each document-based asset shall be endorsed by using the header and footer facility, by hand or, by using an appropriate stamp. Functions will make blank forms/templates relevant to their area of the business on their respective portal sites.

A standard 3 column footer will be used on all documentation. The left-hand column should carry the name of the Service, the version number of the document and the date of latest issue. The centre column should state the security classification assigned to the document. All pages shall be numbered in the right-hand column formatted as 1 of 9, 2 of 9, etc.

The category 'Official' could apply to a wide range of assests. In some circumstances, where there is a clear and justifiable requirement to further restrict access to an asset, that asset should be marked OFFICIAL-SENSITIVE. In such cases, identifying the nature of the sensitivity will be useful, so a further descriptor should be added. For example, OFFICIAL–SENSITIVE (SLT) OFFICIAL-SENSITIVE (PERSONAL) or OFFICIAL–SENSITIVE (FINANCE).

Documents may be received from outside the Service which are protectively marked contrary to this Information Classification Policy as the originating organisation may apply a different classification/protective marking scheme. Those markings can, however, be used to assess how the documents should be handled. For example, a document marked “Commercial in Confidence” may be treated as “OFFICIAL–SENSITIVE (FINANCE)” and a document marked “Addressee Only” may be treated as “OFFICIAL–SENSITIVE (PERSONAL)”. If in doubt, contact the Corporate Assurance Section for advice.

## 8. STORAGE & HANDLING

All assets that are protectively marked must be stored and handled in accordance with the assigned classification. Care should be taken with protectively marked information assets when uploading them to a SharePoint site or other information stores, to prevent unauthorised disclosure. Where information assets have a protective marking, it is the responsibility of the author to ensure they are not available for general browsing or returned in search results by those without a legitimate need to access them. The Digital Services Section can advise of how this can be best achieved.

Details of handling procedures are contained at Appendix B.

Staff should also refer to the Service’s Records Management and Data Quality Policy.

## 9. SECURITY & ACCESS

Users shall, as far as possible, operate a clear-desk and clear-screen policy, requiring all protectively marked assets to be locked away when the desk or computer workstation providing access to the asset is unattended. Further details on the handling of assets are contained at Appendix B. All offices and storage locations holding protected assets shall have secure storage.

When an asset is passed from one location to another, the responsibility for ensuring the security of that asset shall also pass with it.

The Service shall consider each role, rather than the individual, to determine appropriate levels of access to assets and adopt the principle of least privilege. This access level is to be recorded on every role profile, together with the corresponding security vetting level required by the post holder.

Secret or Top-Secret assets should only be accessed by persons cleared to at least ‘Security Check’ (SC) level, as defined in the Government’s Baseline Personnel Security Standard (BPSS).

Staff must not expose any information asset classified as Official or higher to any non-corporate communication channel (eg WhatsApp, private e-mail, SMS or other social media platform).

## 10. ARCHIVING

When assets are archived, the classification shall be formally reviewed and, if necessary, re-graded. If a document is downgraded, this may result in the conditions for storage and disposal being less stringent. The Service's Disposal and Destruction of Records Policy Delivery Guidance provides more details.

## 11. DISPOSAL

All information assets must be disposed of in accordance with the Service's Disposal and Destruction or Records Policy Delivery Guidance, and the guidance in Appendix B.

Briefly:

- All 'Official' paper assets must be disposed of to prevent reconstruction (e.g. by cross cutting shredders, incineration or pulping). All electronic assets will be dealt with by Digital Services, including by wiping and/or destruction of storage media.
- Secret or Top-Secret assets must be disposed of following consultation with the Corporate Assurance Section.

## 12. MONITORING & AUDIT

Procedures will be implemented to ensure auditing and random integrity testing of processes and systems of the Service.

**If anyone requires any further guidance / information regarding this document, please contact Corporate Assurance**

## APPENDIX A - INFORMATION CLASSIFICATION

Information Classification is one of the building blocks for the Information Security Management System. The purpose of this document is to establish an information classification framework to guide members of the Service in using and managing information in the scope of their work.

| Information Category | Description | Examples |
|---|---|---|
| **Not Protectively Marked** | Information that the Service has published for general or public consumption, or publicly known information that the Service has received from another organisation.<br><br>Basic security is needed to ensure the integrity of Service information. | • Information contained within the Freedom of Information Act Publication Scheme.<br>• Leaflets and Brochures<br>• Websites<br>• Fire Authority Reports and Minutes<br>• Financial and Performance Information<br>• Published Internal and External Audit Reports<br>• Press Releases<br>• Service Policies |

| | | |
|---|---|---|
| **Official** | Information, which is sensitive, not for disclosure to the public and needs to be protected,but does not have a national security dimension.<br>Compromise of the information would likely:<br>• cause financial loss or loss of earnings potential to, or facilitate improper gain or advantage for, individuals or companies;<br>• prejudice an investigation or facilitate the commission of crime;<br>• disadvantage the Service in commercial or policy negotiations with others;<br>• pose a reputational risk to the organisation;<br>• cause substantial distress to an individual or, group of individuals;<br>• breach proper undertakings to maintain the confidence of information provided by third parties, or<br>• breach statutory restrictions on the disclosure of information.<br><br>Where classification is necessary, this is the most likely classification for any document that the author is writing.<br><br>Where it is felt access ought to be restricted to only certain people, consider marking as Sensitive and adding who should be able to see it, as the descriptor (e.g., Finance, SLT, Personal). | • Tactical plans for specific premises<br>• Major incident plans<br>• Town centre evacuation plans<br>• Fire safety files<br>• Personal information that could be used foridentity theft<br>• Personal information regarding medical ordisciplinary information<br>• Exempt Fire Authority Reports<br>• Passwords and information on security procedures<br>• Personal record files<br>• Payroll information including pay and deductions<br>• Conduct and Performance records<br>• Occupational medical information<br>• Vulnerable person details exchanged with otheragencies<br>• Sickness and other absence information<br>• Locations of sensitive material or plant used tosupport Business Continuity<br>• Contracts and other legal documents and material<br>• IT/IS Network diagrams, IP addresses and information about sensitive network segments andsystems<br>• Proprietary and in-house software source code<br>• Information subject to a non-disclosure agreement |

| | | |
|---|---|---|
| **Secret** | The compromise of this information or material would likely:<br>• damage diplomatic relations (i.e. cause formal protest or other sanction);<br>• to prejudice individual security or liberty;<br>• cause damage to the operational effectiveness or security of UK or allied forces or the effectiveness of valuable security or intelligence operations;<br>• work substantially against national finances or economic and commercial interests;<br>• cause substantial material damage to national finances or economic and commercial interests.<br>• substantially, to undermine the financial viability of major organisations;<br>• impede the investigation or facilitate the commissionof serious crime;<br>• impede seriously the development or operation of major government policies;<br>• shut down or otherwise substantially disrupt significant national operations;<br>• raise international tension;<br>• damage seriously relations with friendly governments;<br>• threaten life directly, or seriously prejudice public order, or individual security or liberty, or<br>• cause serious damage to the operational effectiveness or security of UK or intelligence operations. | • Intelligence reports.<br>• Information received from the Counter Terrorism Unit Fire Liaison Officer relating to the threats to National Security<br>• Information received from the Counter TerrorismUnit Fire Liaison Officer relating to specific identified threats, incident or individuals<br>• Marauding terrorist attack (MTA) incidents/reports |

| | | |
|---|---|---|
| **Top Secret** | The compromise of this information or material would likely:<br>• threaten directly the internal stability of the UK or friendly countries;<br>• lead directly to widespread loss of life;<br>• cause exceptionally grave damage to the effectiveness of extremely valuable security or intelligence operations;<br>• cause exceptionally grave damage to relationswith friendly governments, or<br>• cause severe long-term damage to the UK economy | Already marked Top Secret |

## Questions to ask when determining the classification level

In order that staff can determine which level of classification to assign to a document or asset, the following questions should be used as a guide. In simple terms, the furthest point down the list where the answer to a question is yes, determines the classification needed. It should be remembered though that authors shall avoid the over-classification of assets, as this means that the intended target audience may be unable to access the asset or, that it cannot be transmitted. If there is any doubt, then seek advice from the Corporate Assurance Section, and in the meantime classify the document at the higher level until a decision has been made.

| Is the answer yes to any of the questions in each box? | If so, then the classification is the one listed here |
|---|---|
| • Is the information published for general or public consumption?<br>• Is it publicly known information that we have received from another organisation?<br>• Is it something we would send to a member if the public if they asked to see it? | Not protectively marked |
| • Could it be used for identifying theft?<br>• Could a commercial company use it for improper gain, for example contract financial details about a supplier?<br>• Would an individual, or group of individuals be very distressed if it was shared?<br>• Would it breach the law regarding disclosure of information and/or data protection legislation?<br>• Could it damage the reputation of the Service if it were lost or accidentally published? | Official |
| • Could it be used to undermine military operations?<br>• Could it be used to effect national security?<br>• Could it be used to impede government policies?<br>• Could it seriously affect the management of a public sector agency (HFRS included)?<br>• Could it harm a police enquiry?<br>• Has it been classified as Secret by a government department?<br>• Could it damage international diplomatic relationships?<br>• Could it damage national security, military or intelligence operations?<br>• Could it affect national finances?<br>• Could it be used to facilitate a serious crime, or impede a police investigation into one?<br>• Could it be used to shut down, or seriously affect, significant national operations? | Secret |
| Has it been classified as Top Secret by a government department? | Top Secret |

## APPENDIX B – HANDLING PROCEDURE

| | Not Protectively Marked | Official | Secret | Top Secret |
|---|---|---|---|---|
| **Portal / Web Storage** | Unrestricted | Contact Digital Services, your SharePoint champion or Corporate Assurance who can advise on secure storage. | Not to be used. | Not to be used. |
| **Physical Storage** | Unrestricted. | Stored in any lockable furniture.<br><br>Not to be taken off site unless it can be guaranteed the asset will either not be left unattended or will be locked awayin lockable furniture. | Double locked within a secure environment, e.g. locked cabinet within a locked room. Not to be taken off site without permission of the originator. | Double locked within a secure environment, e.g. locked cabinet within a locked room. Not to be taken off site without permission of the originator |
| **Electronic Storage** | Unrestricted. | Files stored on computer hard drives, CD, memory stick or other electronic media must be marked with the security classification of the most highly classified data stored on the device. Files can be saved on mobile phones, tablets and laptops if they are secured with a password. If held within an email on a mobile phone must be also secured with a password.<br><br>MDTs are suitable for this type of storage.<br>Any Digital Services Equipment that is lost and contains such files,the user must contact Digital Services immediately to report the loss asthey have the ability to remotely wipe the device. | Files to be located on File Servers and password protected. | Files to be located on File Servers and password protected. |
| **Clear Desk** | Unrestricted use. | Must not be left unattended during working hours when away from desk and unable to lock office. | All documents to be locked out of sight when desk not attended. | All documents to be locked out of sight when desk not attended. |

| | Not Protectively Marked | Official | Secret | Top Secret |
|---|---|---|---|---|
| **Post / Courier Dispatch** | Sealed in envelopes. | Address the envelope to an individual name or job title and mark it 'Addressee Only'.<br><br>Do not include classification on the envelope.<br><br>Include return address. | Not to be sent. | Not to be sent. |
| **e-mail (including mobile devices)** | Unrestricted use. | Unrestricted use in most cases, but consider use of password protection for attachments. Where a password protected document is transmitted, the password must not be contained in the same e-mail.<br><br>OFFICIAL-SENSITIVE (PERSONAL) must be commercially encrypted. Seek advice from Head of Digital Services.<br><br>If sending to external recipient, validate the recipient address prior to transmission. | Not to be sent. | Not to be sent. |
| **Telephone (including cordless, mobile, Airwave** | Unrestricted use. | Unrestricted use. | Not to be used. | Not to be used |
| **Copying / Printing** | Unrestricted use. | Unrestricted use, but if using a shared printer, printing must be to Secure User Box. | No copies to be made. | No copies to be made. |
| **Fax** | Unrestricted use. | Must only be faxed when the recipient has confirmed that they are at the fax machine ready to personally receive the fax. | Not to be used | Not to be used |

| | Not Protectively Marked | Official | Secret | Top Secret |
|---|---|---|---|---|
| **Disposal** | Any appropriate means, including general recycling for wastepaper. | Use cross-cut shredder or put documents in a confidential waste sack and arrange collection by Stores.<br><br>Confidential waste sacks should secured when offices are unattended. | Cross-cut shredder or, one with an appropriate security classification. Shred by placing the paper in at right angles to the print. The width of the shredded strips should not be more than 4 mm and not show more than two characters side by side. Place them in a confidential waste sack to be collected by an approved waste collector.<br><br>Keep a record of the date the document was destroyed and who authorised it.<br><br>Records must be kept up to five years. | Cross-cut shredder or, one with an appropriate security classification. Shred by placing the paper in at right angles to the print. The width of the shredded strips should not be more than 4 mm and not show more than two characters side by side. Place them in a confidential waste sack to be collected by an approved waste collector.<br><br>Keep a record of the date the document was destroyed and who authorised it.<br><br>Records must be kept up to five years.<br><br>There must be two people witnessing the shredding and signing the authorisation |

When dealing with organisations that do not employ the Government Security Classifications (Jun 2023) you must alert them to the special handling requirements necessary for protectively marked assets. This can be done by using Information Sharing Agreements, data processing agreements, non-disclosure agreements or confidentiality letters.

In all cases, bulk transfers of information should be avoided where possible to share the minimum of data which is needed.