

**ORDER NO. 1/XX**  
**WEST MIDLANDS FIRE SERVICE**  
**MANAGEMENT OF INFORMATION**

## **1. STRATEGY**

It is the strategy of the West Midlands Fire and Rescue Service to manage its information assets to facilitate access to accurate, reliable and timely information in order to support its core activities and legislative obligations.

The government has laid down clear guidance through the Cabinet Office about how this is to be achieved within its framework document [Her Majesty's Government Security Policy Framework \(HMG SPF\)](#). Information is a key strategic asset and through appropriate governance and management can lead to efficiencies and better decision making. The Strategic Enabling Team (SET) are responsible for information assets in their respective areas and must be involved with decisions to release information.

The organisation will identify its information assets and create an Information Asset Register (IAR) to risk assess and classify information to ensure it is adequately protected.

The IAR will be available to enable accurate classification of information assets.

The Brigade will promote a culture of openness and accountability and where possible will publish information electronically on the Brigade [website](#)

The Authority will ensure that requests for information are responded to promptly and in line with relevant legislation.

Management of Information includes Classification and Marking, Requests for Information, Data sharing and Handling Instructions - See Appendix 1 for overarching Management of Information Flowchart

## **2. PROCEDURES**

The role of Senior Information Risk Owner (SIRO) is held by the Deputy Chief Fire Officer with responsibility for information security within West Midlands Fire Service.

The SIRO role is supported by the information Asset Owners (IAO) who are the Strategic Enabling Team (SET) with responsibilities for information assets within their respective areas.

### **2.1 CLASSIFICATION AND MARKING**

The Government classification Scheme (GCS) is the overarching framework that defines how information assets should be protected. There are three levels of classification **OFFICIAL**, **SECRET** and **TOP SECRET**.

There will be a very limited amount of information within the organization that will be marked SECRET or TOP SECRET and they are likely to be documents that have originated from partner agencies such as West Midlands Police. The originator of this category of information will specify their data handling instructions prior to dispatch of this information.

Within this new classification system, unless explicitly stated, all WMFS information is classed as OFFICIAL and WMFS systems are deemed appropriate to adequately protect OFFICIAL information.

There are no plans to retrospectively mark documents within the organization.

### 2.1.1 OFFICIAL

This new system replaces all previous systems of classification such as PROTECTED, RESTRICTED and CONFIDENTIAL.

Each organisation will have its own labels with its own handling instructions with no predefined meaning to the labels.

The following labels have been approved by the Strategic Enabling Team (SET) for use within WMFS.

**OFFICIAL - WMFS PUBLIC** – Information that can be published openly on the Internet and released without restriction into the public domain

E.g. A Published copy of The Plan, Information about becoming a volunteer, Community Open days at fire stations

**OFFICIAL – WMFS LOW** – Information that if released would cause annoyance or inconvenience to individuals or the organisation but no potential physical, financial or other distress or damage.

E.g. Purchase order for office furniture, schedule of vehicle maintenance

**OFFICIAL – WMFS MEDIUM** – Information that if released would cause distress to individuals, cause financial loss or improper gain, prejudice the investigation or facilitate the commission of crime or disadvantage the organisation in commercial or policy negotiations with others. It may be protected under legislation e.g. Data Protection Act 1998

E.g. Occupational Health report about an individual, details of vulnerable people,

**OFFICIAL – WMFS HIGH** – Information that if released or compromised would cause significant distress to individuals, compromise law enforcement and resilience arrangements and impede the ability of the organisation to perform core functions such as responding to incidents.

E.g. Access to the mobilising system.

This new system allows greater flexibility to enable organisations to manage their information using their own naming standards and handling instructions to suit the requirements of the organisation. However, this does mean that:

- People outside the brigade will not understand what these labels mean; and
- Other organisations may use the same labels but have completely different meanings and handling instructions.

Therefore, you will note that our labels all have 'WMFS' in them to help distinguish our labels from other organisations' labels.

It is important that:

- You label all information correctly;
- You understand and follow WMFS handling instructions - see Appendix A
- You provide handling instructions for recipients of your information e.g. Recipient only – no onward forwarding without permission;
- You understand and follow handling instructions provided by others e.g. *OFFICIAL – WMFS HIGH* may differ from another organisation's definition of OFFICIAL -HIGH;
- You check with information originator if no handling instructions are received.

When classifying information, a risk assessment should be undertaken to consider the likely impact if the asset were to be compromised and assisting with determining the correct level of marking required.

### 2.1.2 MARKING OF DOCUMENTS AND OTHER MATERIAL

This is applicable to both paper and electronic documents such as reports, spreadsheets and presentations, handwritten notes and other unstructured data.

The presence of a protective marking does not mean that the material should not be disclosed in appropriate circumstances (*e.g.* to other agencies involved in joint operations or the release of personal data to data subjects under the provisions of the Data Protection Act 1998).

Conversely the absence of a protective marking does not mean that a document should be made freely available or published. The above definitions of OFFICIAL – WMFS PUBLIC, OFFICIAL – WMFS LOW, OFFICIAL- WMFS MEDIUM and OFFICIAL- WMFS HIGH should be applied to assess the risk to the information contained within it and appropriate protective measures applied assess the risk to the information contained within it and appropriate protective measures applied.

Protectively marked electronic medium such as DVDs, USB devices and DVDs are to be treated in the same way as other documents. They must be visibly marked and numbered and all other measures are to be implemented

- Protective markings must be clear so that the value of material is clearly conveyed to those who handle it. Each page must be marked at both the top and the bottom with the correct security marking;
- blank pages within classified material must be marked with the legend 'intentional blank page' apart from those classified as OFFICIAL – WMFS PUBLIC as these documents do not require this level of protection;
- all pages within a protectively marked document must be given consecutive page numbering apart from those classified as OFFICIAL – WMFS PUBLIC as these documents do not require this level of protection;

Thought must be given to limiting the number of copies produced.

## 2.2 REQUESTS FOR INFORMATION

There are two main pieces of legislation that enable the requesting of information from the organisation.

The Freedom of Information Act 2000 gives people the right to request information from public authorities and is intended to promote a culture of openness, transparency and accountability amongst public sector bodies and enable the public to better understand how public authorities carry out their duties, how they make decisions and how they spend their money.

See Appendix 2 for further information about the Freedom of Information Act 2000.

The Data Protection Act 1998 gives data subjects the right to access personal information that the Brigade may hold about them. A data subject may be a service user, an employee including temporary and volunteers and the communities that we serve.

See Appendix 3 for further information about the Data Protection Act 1998.

Other legislation that may facilitate formal access to information is the Environmental Information Regulations 2004 ([See Appendix 4](#)) and the Re-use of Public Sector Information Regulations 2005([See Appendix 5](#))

The process for handling formal requests for information as detailed above is well established within the organisation and these are managed by the Data Management team in ICT.

All FOI requests are published anonymously on the internet in a [Disclosure Log](#)

### 2.2.1 Classification of Requests

Other requests for information that are received that do not fit under the legislation above should be risk assessed and classified in line with the categories above e.g. OFFICIAL WMFS- MEDIUM

The handling procedures for the different categories of information are aligned to the levels that are detailed in the classification scheme.

**OFFICIAL - WMFS PUBLIC** – Requester will be asking for information that is publicly available and should be directed to the website in the first instance as the information will be published and there is no requirement to notify SET member.

**OFFICIAL – WMFS LOW** – Requesters will be requesting routine information whereby there are likely to be established processes such as for IRS report requests from insurance companies and there is no requirement to notify SET member.

**OFFICIAL – WMFS MEDIUM** – Requester will be asking for information that is not routinely available and there is no established process for release. Relevant SET member needs to be consulted to approve or not the release of the information and inform Data Management to maintain a log of requests.

**OFFICIAL – WMFS HIGH** – Requesters will be requesting information that is considered to be operationally critical and the relevant SET member needs to be consulted to approve or not the release of the information and inform Data Management to maintain log of request.

West Midlands Fire Authority will be consulted about requests for information specifically related to the business of the Fire Authority but the responsibility for notification, response and disclosure solely rests with West Midlands Fire Service.

See Appendix 6 for Requests for Information Flowchart

## 2.3 DATA SHARING

As part of collaborative arrangements with partner agencies, the Brigade is a member of many information sharing initiatives and these arrangements are documented and agreed by all participants. These initiatives are described in many differing ways such as Information Sharing Protocol, Data Exchange Agreement, and Data Sharing Agreement but essentially they mean the same and it is a considered means whereby organisations can share data to achieve outcomes. These information sharing agreements provide an invaluable exchange of information related to vulnerable people thus enabling the Brigade to target its resources in the most appropriate areas.

There are established processes for the exchange of information and all employees involved with this work are aware of their roles and responsibilities and are expected to operate within authorised procedures contained within the agreement.

The Information Commissioner's Office has issued a [Code of Practice](#) related to Data Sharing.

The relevant SET member should be involved with the decision to enter into data sharing arrangement with partner agencies but they do not require notification about every item of data that is exchanged.

## 2.4 HANDLING INSTRUCTIONS

Basic security measures must be applied to all organisational information thereby ensuring material is given an agreed level of protection by those who handle it.

Material should not be over or under-classified as this may prevent effective use of the information within the organisation.

- Organisational information should be handled in line with the guidance provided in Appendix A;
- the distribution of organisational material should be confined to those with a genuine 'need to know';
- the originator should review protectively marked documents with a view to downgrading or destroying them e.g. documents that are subsequently published on the Intranet should be marked as OFFICIAL –WMFS PUBLIC.

#### 2.4.1 Physical storage

Protectively marked material should be stored in a secure environment (which is defined as 'a barrier, or combination of barriers, providing protection appropriate to the risk of compromise') as follows.

- **OFFICIAL – WMFS PUBLIC:** material may be freely distributed and published externally;
- **OFFICIAL- WMFS LOW:** material should be protected by one level of protection (e.g. Proximity pass for access to the building and appropriate areas)
- **OFFICIAL – WMFS MEDIUM:** material should be protected by two levels of protection (e.g. a locked container within a building with access controls). Effective control systems must be in use to ensure that access is limited to those who need access to the material.
- **OFFICIAL – WMFS HIGH:** material should be stored in a purpose built storage room with restricted access. Where an IT system is used to store protectively marked data, physical security measures should be taken to secure all of its components. Removable parts of IT systems, such as removable hard drives, should be stored in the way appropriate to the protective marking of the data they contain.

#### 2.4.2 Destruction of documents

- **OFFICIAL – WMFS PUBLIC:** no requirement to control disposal or destruction of documents;
- **OFFICIAL- WMFS LOW:** all documents to be disposed of in line with the organisational policy related to the retention and disposal of records
- **OFFICIAL- WMFS MEDIUM and OFFICIAL-WMFS HIGH:** all documents to be shredded.

#### 2.4.3 Destruction of other material

- **OFFICIAL – WMFS PUBLIC:** no requirement to control disposal or destruction of material;

Material that is protectively marked **OFFICIAL – WMFS LOW, OFFICIAL - WMFS MEDIUM** and **OFFICIAL – WMFS HIGH** and is stored on magnetic media should be destroyed by the following methods:

- CDs and DVDs containing such data may be destroyed by dismantling the casing and cutting the disk itself into at least quarters; the fragments may then be treated as normal waste.
- Data should be securely erased by ICT if the system is being reused within the authority,
- If the system is being disposed of external to the organization then the ICT team should have appropriate processes and procedures in place to ensure that the data is securely erased and assurance is received to confirm this.

#### 2.4.4 Time limited classification

The degree of sensitivity of information often decreases over time, e.g. when consultation has closed and a policy has been formulated. Once this has occurred the IAO may want to downgrade or remove restrictions altogether.

#### 2.4.5 Markings from other government agencies and international organisations

Many governments and some international organisations (e.g. NATO) have classification systems similar to this one. Agreements often exist for the mutual recognition and protection of marked documents.

In all cases, staff are required to provide the level of protection indicated by the originator. In some cases international organisations use the word 'restricted' to mean 'for official use only'. If any doubt exists about how any such information should be treated, a check should be made with the originator.

#### 2.4.6 Movement

If protectively marked material classified as **OFFICIAL – WMFS LOW** or above is being carried in a public place, it must be kept under cover with no outward indication of the contents. The material must not be left unattended and outside the immediate direct control of the carrier at any time.

When carrying protectively marked material, all items must be treated according to the highest marking.

#### 2.4.7 Royal Mail and courier services

It should be noted that all undeliverable Royal Mail is forwarded to Northern Ireland to be processed and this could, in extreme circumstances, lead to a breach of security. Where there is a risk of compromise ensure a return address is shown on the back of the envelope.

When sending protectively marked material within Great Britain by Royal Mail or courier services the following rules apply:

- **OFFICIAL- WMFS PUBLIC, OFFICIAL – WMFS LOW and OFFICIAL-MEDIUM** material may be sent by ordinary post. It must be sent in a sealed envelope with no protective marking visible (except '**PERSONAL**', where appropriate).
- **OFFICIAL – WMFS HIGH** material should not be sent by ordinary post.

#### 2.4.8 Telecommunications

##### 2.4.9 Answerphones and voicemail

Answerphones, voicemail or any other answering service should not be used for protectively marked information above **OFFICIAL- WMFS LOW**.

##### 2.4.10 Mobile telephones

Mobile phones offer some degree of protection when used as radio transmissions between the handset and the base station are encrypted. However, when a call is passed onto another base station within the network, or to the main telephone network, it is not encrypted. Care should be taken when passing information higher than **OFFICIAL- WMFS MEDIUM**.

##### 2.4.11 Radio systems

The Airwave system is encrypted and capable of carrying traffic up to (and including) **OFFICIAL- WMFS HIGH**. However, all users should be aware that

transmissions may still be heard by other authorised users of the Airwave system (for example, fire and rescue service staff throughout the country who are monitoring the relevant talkgroup) Therefore, suitable precautions must still be taken to ensure the confidentiality of radio transmissions.

Fireground radios should only be used to pass information **OFFICIAL – WMFS PUBLIC** and **OFFICIAL - WMFS LOW**.

The Emergency Services Network (ESN) will replace the current Airwave system and will be capable of carrying traffic up to (and including) **OFFICIAL- WMFS HIGH**.

#### 2.4.12 Message pager systems

Message pager systems are inherently insecure and can easily be intercepted. It should only be used to carry information of level **OFFICIAL – WMFS PUBLIC** or **OFFICIAL – WMFS LOW**.

#### 2.4.13 Working away from authority premises

The home environment is usually less secure than the controlled environment of the organisation's premises. Protectively marked documents or removable media of **OFFICIAL – WMFS HIGH** must not be taken home nor may it leave authority premises.

Permission to work at home on protectively marked material up to and including **OFFICIAL – WMFS MEDIUM** may be given by a member of SET. Caution and discretion must be used and it is the responsibility of the end user to protect the information.

## 2.5 MONITORING

When FOI requests are received in the organisation, SET members are made aware of the request for information. The details of the requester are not disclosed to the SET member in line with the Information Commissioner's guidelines related to FOI requests being 'applicant blind'

SET will receive a monthly report to provide detail about FOI requests and informal requests for information at level received within the month.

Information Sharing Agreements are reviewed periodically and most will stipulate that an audit trail is kept of disclosures under the agreement. This contributes to assessing the effectiveness of the arrangements and the value to the Brigade.

## 3. SYSTEMS

New systems are being designed to facilitate access to all organisational information and will respect the classification of the material and protect it both in transit and at rest in terms of confidentiality, integrity and availability.

In the interim there is a personal accountability to ensure that information is adequately protected in line with this framework and any other overarching legislation that is applicable e.g. Data Protection Act 1998.

Electronically stored documents and e-mail attachments of **OFFICIAL - WMFS MEDIUM** and **OFFICIAL - WMFS HIGH** may be e-mailed within the authority i.e. between *wmfs.net* and *wmfs.net* e-mail addresses, but must **not** be e-mailed outside the internal IT network unless via a secure network such as the Criminal Justice Secure Email (CJSM) system. Further advice about using this system should be sought from ICT.

Organisational information classified as **OFFICIAL – WMFS MEDIUM** or above should not be stored on personal devices or within other cloud storage services that are not part of WMFS provision.

#### **4. IF YOU REQUIRE ANY ASSISTANCE WITH ANY ASPECT OF THIS FRAMEWORK THEN PLEASE CONTACT THE DATA MANAGER.CROSS REFERENCES**

Information Commissioner's Office website [www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk).  
Local Government Transparency Code 2014

#### **5. KEY CONSULTEES**

To be arranged

#### **6. EQUALITY IMPACT ASSESSMENT**

An Equality Impact Assessment was not necessary as there is no impact on people.

#### **7. OWNERSHIP**

This order has been approved by SET.

#### **8. RESPONSIBILITY AND REVIEW/AMENDMENT**

##### **8.1 Responsible Corporate Board Member/Department**

SE ICT/SIRO – Deputy Chief Fire Officer

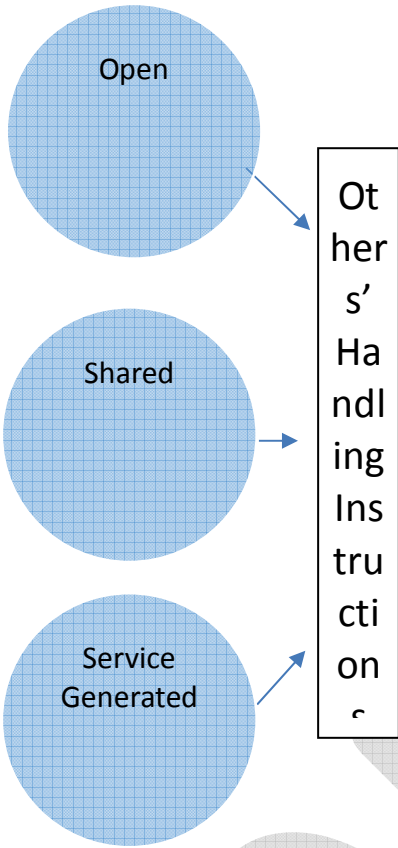
##### **8.2 Created/fully reviewed/amended**

This Order has been created by the Data Manager in October 2016

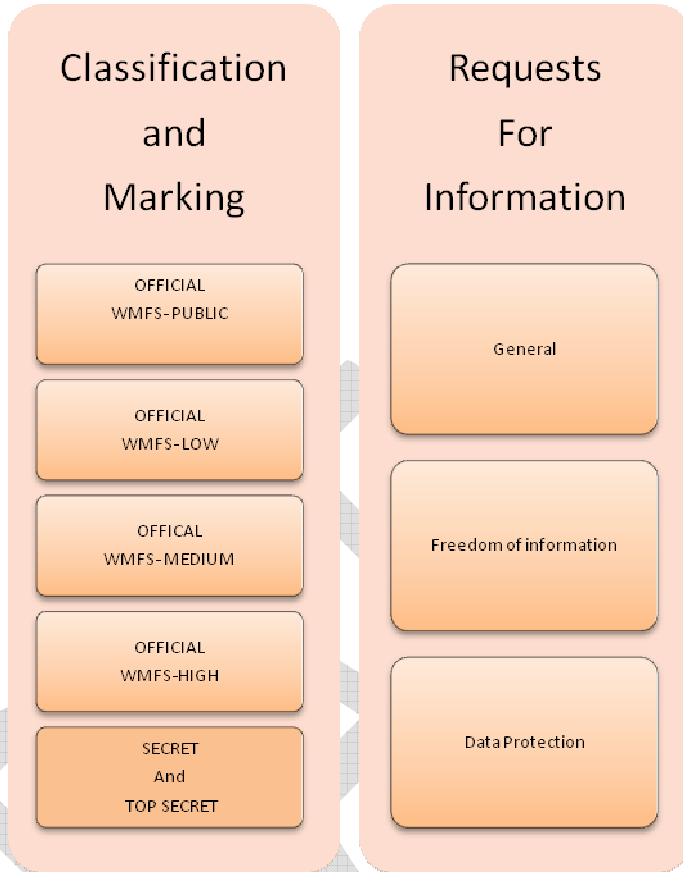


# APPENDIX 1

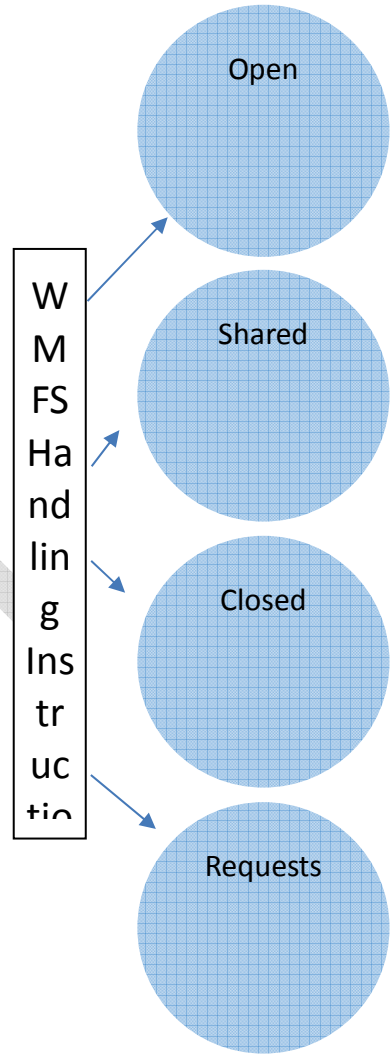
## Data Inputs



## Processing



## Data Outputs



## APPENDIX 2

# FREEDOM OF INFORMATION ACT 2000

## 1. PROCEDURES

The Freedom of Information Act 2000 gives people the right to request information from public authorities and is intended to promote a culture of openness, transparency and accountability amongst public sector bodies and enable the public to better understand how public authorities carry out their duties, how they make decisions and how they spend their money.

The main features of the Act are:

- A general access to information held by public authorities.
- A duty on public authorities to adopt publication schemes.
- Exemptions from the duty to provide certain categories of information.
- A requirement on public authorities to exercise discretion and balance the requirement to provide information with a duty to withhold it (the 'public interest test').
- Arrangements in respect of costs and fees.
- Arrangements for enforcement and appeal.
- Guidance within Codes of Practice.

A requirement of the Act is for each public authority to produce and maintain a 'Publication Scheme'. The Publication Scheme sets out what information is already available in a set format how that information can be requested and whether there is a charge for providing that information.

The Authority's [Publication Scheme](#) is published on the [Brigade](#) website and on the Intranet.

It is the responsibility of the Data Manager to maintain and update the scheme.

### 1.1 Rights of access

Any person making a request for information to a public authority is entitled to be informed in writing by the public authority whether it holds information of the description specified in the request and to have that information communicated.

This is commonly described as 'the duty to confirm or deny that information is held, and to provide it'.

There are six reasons why a public authority may not have to meet this provision.

- 1) Where it is possible that further information is needed before the request can be answered.
- 2) An exemption applies.
- 3) The public interest in maintaining the exemption outweighs the public interest in disclosing the information.
- 4) When any fee is charged, and that fee is not paid within three months of fees notice being issued.
- 5) If the public authority estimates the cost of complying with the request would exceed the 'appropriate limit'.
- 6) If the request is vexatious or repeated.

Under some exemptions, certain conditions have to be met before the duty to confirm or deny is not applicable. The duty to confirm or deny does not arise when information is already accessible or when information is intended for future publication.

## 1.2 Requests for information

A request for information is 'a request which is in writing, states the name of the applicant and an address for correspondence, and describes the information requested.'

There are three essentials that have to be met by anyone requesting information under the Act:

- 1) Put it in writing.
- 2) Name and address of applicant (email address is acceptable).
- 3) Description of the information requested.

Some other features of requests for information are:

- A request is treated 'as in writing' where the text is transmitted electronically and is received in legible form. It should also be capable of being used as subsequent reference by the Authority.
- The applicant does not have to mention the Act itself when making the request.
- An applicant has to identify him/herself for the purposes of the request, but the identity of the applicant is of no concern to the Authority except in the case of vexatious or repeated requests and personal information (see paragraph 3.4).
- The applicant need not be a United Kingdom national or resident. A request can be made by anybody, anywhere in the world.
- There is no restriction on the reasons why the information is being requested and the Authority cannot make enquiries as to why the information is being sought or what it will be used for.
- The Authority can request further information from the applicant in order to identify or locate the information.
- There are no formal requirements on applicants to describe the information in a certain way, e.g. by reference number, but the description has to be sufficient to be able to locate and identify the information.
- The information communicated to the applicant has to be the information held at the time the request was received. Account may be taken of amendments or deletions that would have been made in the normal course of events.
- The Authority must help the applicant to frame a request for information if they are not able to do so on their own, for example, writing down a request on the telephone and then confirming with the applicant the contents of the request are accurate.
- As soon as verification of the request is received the Authority has 20 working days to comply with the request.

Each Authority can decide whether to charge for providing information that will satisfy the request, for example if there are substantial administration costs to gather and reproduce the information.

If a request for information is received in a department, section or on a station it must be date stamped and forwarded immediately for the attention of the Data Manager, Data Management section, marked 'Freedom of Information Request'.

The Data Manager will be responsible for recording the request, obtaining the information from the relevant department, charging any appropriate fees and ensuring that the request is answered within the timescale.

The Data Manager will liaise with the appropriate section or department concerned for assistance in providing the information requested. It is imperative that information is provided in a timely manner to ensure that the specified timescales are met.

The Data Manager may contact you for information about your station, section or team: it is essential that you provide the information as requested – **you must not withhold information because you do not agree with the request, or feel it is unfair.** You can highlight your concerns with the Data Manager upon providing the information, who will determine whether an exemption may apply.

For each request received the relevant SET member will be notified of the request. *There may be some requests for information that are routinely published on the Brigade website and it is not necessary to notify SET members of these requests.*

A monthly report will be produced by Data Management and distributed to all SET members for awareness.

Requests specifically relating to the fire authority will be handled in line with the process above and liaison will occur with authority members through an agreed process.

### **1.3 In line with best practice, anonymised requests will be published in a Disclosure Log on the Brigade website to further promote openness and transparency. Important legislation to consider**

The Freedom of Information Act 2000 needs to be considered in conjunction with the Environmental Information Regulations 2004. Both sets of legislation aim to encourage more open and accountable government by establishing a general statutory right of access to official records and information held by public authorities.

This complements and is influenced by the Data Protection Act 1998, as generally information which involves, or can identify an individual is exempt. However some information relating to more senior employees within the organisation such as the salary is published routinely on the internet as part of the government's local transparency agenda.

Any request for information needs to take into consideration the requirements of all three pieces of legislation. All requests of this nature must be forwarded to the Data Manager at Headquarters who will establish what legislation any request may come under, and provide a formal response.

#### **1.3.1 Exemptions**

Under Freedom of Information, there is a presumption of openness, irrespective of the date of the information, unless an exemption applies. There are two categories of exemptions:

- 1) Public interest – those in which the public authority seeking to reply on the exemption has to establish that the public interest in maintaining the exemption outweighs the public interest in disclosing information.
- 2) Absolute – where no public interest test is required.

There are a number of exemptions to providing data under the Freedom of Information Act but the main ones most likely to apply are:

- Already accessible – Absolute.
- Information intended for future publication – Absolute.
- Information provided in confidence – Absolute.
- Law Enforcement – Public Interest.
- National Security – Public Interest.
- Commercial Interests – Public Interest.

The Data Manager will advise on the full range of exemptions if required and will consider whether an exemption applies on receipt of a request for information under the Freedom of Information Act.

DRAFT

# APPENDIX 3

## DATA PROTECTION ACT 1998

### 1. PROCEDURES

West Midlands Fire Service fully endorse and adhere to the principles of the Data Protection Act 1998.

The Service regards the lawful and correct treatment of personal information as very important to successful service delivery and to maintain confidence between service users, employees including temporary staff, volunteers and those communities we serve. The Service is committed to respecting all rights of those individuals whose personal data it processes and will ensure personal information will be treated lawfully and correctly in accordance with the legislation. It will adopt best practice as designated by the Information Commissioner's Office where possible.

The Service has defined a number of distinctive roles to manage data protection.

Role Title	Position in the Organisation
Data Protection Officer	Data Management Officer
Information Asset Owner (IAO)	SET member from each function responsible for data management within their respective function. Also to be the liaison point for the Data Protection Officer.
Data User	All those that handle data. All individuals have a responsibility to ensure the integrity of the data they use.

Each employee or potential data user will be given such information, instructions and training as is necessary in order to ensure that they are aware of their contractual responsibilities in relation to personal data and so that they are aware that they can, in some cases, be held personally responsible if any personal data is improperly disclosed, destroyed or obtained.

The Data Protection Officer has responsibility to co-ordinate the Service's response to the Data Protection Act 1998 and the Freedom of Information Act 2000, to ensure that the provisions of the legislation are met.

The IAO will have overall responsibility for the personal data kept within their particular department to ensure that such data is maintained in accordance with the principles of the Data Protection Act 1998. This does not absolve Data Users from their responsibility of ensuring that personal data is maintained in accordance with these principles.

#### 1.1 Scope of personal data

##### Definition of Personal data or information

- Is any information held electronically (including all emails) or manually – which relates to a **living** individual who can be identified:
  - from the information ;
  - from the information combined with other information which is in the possession of the Service or is likely to come in to the possession of the Service; or
  - includes any intentions or opinions the Service may have towards the individual.

## **Sensitive Personal data**

The Data Protection Act 1998 defines sensitive personal information as information related to:

- Racial or ethnic origin;
- Political opinions;
- Religious or other similar beliefs;
- Membership of trade unions;
- Physical or mental health or condition;
- Sexual life; and
- Convictions, proceedings and criminal acts

(See Appendices 1 and 2 for further information)

## **1.2 Personal records**

All information held on a Personal Record File (PRF) will be maintained with a high level of confidentiality and only disclosed to those individuals who reasonably require it as part of their duties.

Files that are maintained locally or within the Occupational Health Unit will comply with the same level of confidentiality.

Information held on a Personal Record File will not be kept for longer than is absolutely necessary and documents will be removed and destroyed in a timely manner following the period agreed below.

### **1.3.1 Computerised Personal Record File**

It is the policy of West Midlands Fire Service that one primary Personal Record File will be maintained for each employee. The information in this file will relate to the individual only and will be maintained by People Support Services (PSS) and the employee in accordance with the Data Protection Act 1998.

Appendix 3 details the information that can be held in the Computerised Personal Record File.

## **1.3 Local Personal Record File**

It is acknowledged that in order to manage locally, certain items of personal information must be retained locally on station or within sections; these include performance, attendance management, training information and Permits to Work. These files must be maintained in accordance with the Data Protection Act 1998.

A Personal Record File can be maintained at the location of the individual but must only contain the items of information as listed in Appendix 3.

These files should be sent back to PSS when the employee ceases employment. If an employee moves temporarily for more than 4 weeks or permanently to another location the file should be forwarded to the other locations clearly marked confidential and addressed to the new line manager. Any movement of files must be conducted under confidential cover in sealed envelopes, with the delivery and receipt recorded.

All information must be kept securely and in confidence.

## **1.4 Employee Access**

### **1.4.1 Personal record file**

All employees under the terms of the Data Protection Act 1998 are entitled to know what personal information the organisation holds about them and how it is being processed. If an employee requires access to their personal record file (PRF) information, the following procedure must be followed.

- Requests should be made in writing to the PSS, giving a minimum of 3 days notice.
- PSS will liaise with the employee to facilitate access,
- The Data Protection Act 1998 gives employees an entitlement to information and not documents

If the employee wishes a third party to be present when viewing the file, for example, a legal or trade union representative, this must be included in the request. Representatives will not be allowed to view the file independently without the explicit written consent of the employee concerned.

Every employee has the ability to view their electronic personal information file. If inaccurate information is found on the system and the employee does not have the access to amend it, details should be forwarded to the PSS who will make the amendments on their behalf.

If line managers wish to view a member of staff's Personal Record File, the procedure described above must be followed where a reason must be provided for needing to view the file.

### **1.4.2 Occupational health records**

Access to occupational health records will follow the procedure described above except that the request to view the records is to be submitted to the Practice Manager, Occupational Health who may need to liaise with the OH Manager or their delegated representative.

### **1.4.3 Other personal records**

Requests to access other personal information that the organisation might hold should be made in writing to the Data Protection Officer at Fire Service Headquarters. The information will then be located and a fee charged if appropriate. If the information contains data about any third parties then the information will be released if it is reasonable to do so in line with the legislation, redacted i.e. personal data removed or a summary of the information provided.

## **1.5 Information released to a third party**

Requests are sometimes received either in writing or via telephone from third parties to release personal information about employees, in all cases written permission of the individual must be given before this information is released, exception to this will be in certain circumstances where requests are made by statutory bodies for information.

### **Sports and Welfare**

Such organisations were previously exempt from the Act, but must now comply, but are not required to register under the Data Protection Act 1998.

Whilst it is not necessary to notify the Information Commissioner of the personal data held, this does not exempt clubs from the first principle of the Act, that is, personal data shall be processed fairly and lawfully.



## 1.6 Requests for information

All other requests for information in whatever form, for example, paper records, computer records, tapes, and so on, should be forwarded through to the Data Protection Officer.

If a request for information is received in a department, section or on a station it must be date stamped and forwarded immediately for the attention of the Data Protection Officer, Data Management Section, marked 'Confidential - Data Protection Request'. If possible, the request should be sent by e-mail.

The Data Protection Officer will be responsible for recording the request, obtaining the information from the relevant department, charging any appropriate fees and ensuring that the request is answered within the timescale. The timescale for response to requests for information is 40 days and the suggested fee is £10 but this is not always charged.

Requests for the disclosure of personal data related to the 'Transfer of Undertakings (Protection of Employment) Regulations' (TUPE) 2006 are the responsibility of PSS department. These need to be in line with TUPE and Data Protection Act 1998 requirements.

The Data Protection Officer will liaise with the department or station concerned for assistance in providing the information requested. It is imperative that information is provided in a timely manner to ensure that the specified timescales are met.

### 1.6.1 Requests for incident information

The Service receives enquiries from solicitors, loss adjusters, insurance companies and other interested parties for details of fires and other Fire Service activities. The intentions of the enquirer are often unknown or liable to change at a later date.

The Service is not entitled to release information about a data subject to any third party without the data subject's consent; there are a few exceptions, for example, data requested by the police to assist them with criminal investigations. Fire Service reports, in particular the Incident Recording System (IRS) Fire Report, contain information about persons involved in incidents and are therefore not to be released by fire stations.

All such requests must be submitted in writing by the party wishing to obtain the information. This is to be forwarded to the Central Administration team at e-mail address InformationDisclosure@wmfs.net. A fee will usually be charged for this information.

### 1.6.2 Release of information for legal proceedings

When the Fire Service is involved in legal proceedings, the Civil Procedure Rules require that all relevant documents shall be disclosed to the other parties involved. This includes all documents which are, **or have been** in the possession, custody or power of the relevant party and which relate to any matter in question between the parties.

A request for such documentation will usually be made by the PSS Section to the relevant section, department or station. This request includes **all** relevant documents, including original or rough notes, and whether they are supportive or potentially damaging, so a thorough search must be made.

In general terms, it is likely that all available documentation is disclosable and therefore, personnel should forward all documents, which will be considered by the Service's advisors before disclosure.

If original documents are forwarded, copies should be taken and preserved by the forwarding party. Where copies of documents are forwarded, care must be taken to ensure the best possible quality copy is obtained.

Stringent time limits are imposed for disclosure of documentation. Hence it is vital that all documents are forwarded, as soon as possible after the request has been made.

### **1.6.3 Definition of documents (legal proceedings)**

As all relevant documentation should be disclosed, it is not possible to provide a definitive list. However, for the purposes of this order, examples include: **all** paper records, written or printed, reports – including IRS and narratives (where provided), internal and external memoranda, accounts, invoices and contracts, any information held on computer or other mode of electronic storage, for example, e-mails, CD-ROM, diagrams, plans, maps, photographs and videos.

It should be noted that the marking of any disclosable document 'confidential' or 'personal' does not necessarily preclude disclosure in respect of legal proceedings.

The requirements of this standing order emphasise the importance of maintaining comprehensive and accurate filing systems, as the implications of non-disclosure of relevant documents are far reaching.

### **1.6.4 Information received or requested from the police about employees**

On occasions, the Service maybe contacted by police officers, who have either requested personal information about employees, or have notified the Service that employees have been arrested or involved in incidents to which the police have been called. The Fire Service is not a 'notifiable occupation' for disclosing convictions of persons for certain employers.

Therefore, the following procedure will be adopted upon receipt of such requests from the police, or where information is received about individual employees:

- where the police request information from a station, the officer in charge should only confirm whether or not an individual is employed at the station;
- any requests for further information about employees should be refused and the requesting police officer referred to the duty principal command officer via Fire Control. The Service will then only release personal details where a serious crime is being investigated or where a warrant has been issued;
- information will only be released after receipt of the police force's standard disclosure form;
- employees are obliged to notify the Service if they have been charged with a criminal offence, (senior officers do not visit police stations if informed by the police that an individual has been detained or questioned whilst off duty). The Service does provide welfare support should individuals require it; this should be discussed with the Line Manager.
- personnel who are being questioned or detained by the Police and who would be unable to report for duty as a result, should request the police to contact Fire Control and inform the duty officer that they will be unable to attend for duty. The duty principal command officer will then be informed and will take appropriate action; and
- requests from the police for copies of recordings from Fire Control will be managed and actioned by Fire Control. The procedure is detailed in Fire Control.

## **1.7 Complaints**

Any complaints must be submitted through the Customer Care and Compliments, Comments and Complaints procedure.

## 1. Schedule 2 Conditions (Data Protection Act 1998)

Schedules 2 and 3 set out specific conditions that have to be met before processing of personal data can take place; these relate to the first of the 8 principles. The conditions are different for sensitive data and non-sensitive data.

Broadly, **non-sensitive data** is not to be processed unless at least **one** of the following conditions has been met:

- the data subject has given their consent to the processing;
- the processing is **necessary** for the performance of a contract to which the data subject is party (the employment contract), or for taking steps to enter into such a contract;
- the Data Controller has to process the information in order to comply with non-contractual legal obligations (such as health and safety obligations);
- the processing is **necessary** to protect the vital interests of the data subject;
- the processing is **necessary** for the administration of justice, exercise of crown functions, or the exercise of any other functions of a public nature exercised in the public interest; or
- the processing is **necessary** for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data is disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

## 2. Schedule 3 Conditions (Data Protection Act 1998)

In the case of sensitive data, processing is permitted only if at least one of the following conditions is met:

- the data is of sensitive personal nature consisting of information as to racial or ethnic origin;
- the individual has given their explicit consent to the processing;
- the processing is necessary for the purposes of exercising or performing any right conferred or obligation imposed by law on the Data Controller in connection with employment;
- the processing is necessary to protect the vital interests of the individual in a case where either the consent cannot be given (incapacity, for example) or else the Data Controller cannot reasonably be expected to obtain consent (for example, the individual cannot be contacted despite various attempts over a considerable length of time);
- the processing is carried out in the course of its legitimate activities by any body or association not established for profit and which exists for political, philosophical or trade union purposes, and which relates only to individuals who are members of that body;
- the individual has already made the information public, by taking deliberate steps;

- the processing is necessary for the purpose of or in connection with legal proceedings, obtaining legal advice or establishing or exercising or defending legal rights;
- the processing is necessary for the administration of justice or exercise of crown functions;
- the processing is necessary for medical purposes and is undertaken by a health professional; or
- the personal data are processed in circumstances specified in an order made by the Secretary of State.

### **Information Commissioner's Office**

The Information Commissioner's Office is the data protection regulator for the United Kingdom. Its responsibility is to publish guidance on and enforce compliance with the Data Protection Act 1998, Freedom of Information Act 2000, Environmental Information Regulations 2004 and the Electronic Information Regulations 2003.

DRAFT

## Principles of the Data Protection Act 1998

### 1 Principle 1 - fair processing

The Data Protection Act 1998 states that the manager cannot hold personal data unless you meet at least one criterion from Schedules 2 and 3 of the Act.

If the organisation does not meet at least one criterion, then there will be in breach of the Act.

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- at least one of the conditions is met; and
- in the case of sensitive personal data, at least one of the conditions is also met.

Any activity whatsoever that involves personal information – held electronically or manually, such as obtaining, recording, holding, disseminating or making available the information, or carrying out any operation or set of operations on the information. It includes organising, adapting, amending and processing the information, retrieval, consultation, disclosure, erasure or destruction of the information. **It is difficult to envisage any activity which does not amount to processing and consideration should be given to conducting a Privacy Impact Assessment (PIA) when embarking on projects and/or activities that may involve processing personal data.**

If the organisation or the employee holds any data that matches any of the above criteria, then they will have to legitimise why they are holding this data. The organisation or employee will also be in breach of the Act if it cannot legitimise the reason for holding the data even if it does match one of the criteria. If data controllers or data users are at all unsure regarding what is a legitimate reason for holding the data, they should seek the advice of the Data Protection Officer.

The processing of data for the purposes of carrying out of 'directed' and intrusive covert surveillance; the use of covert human intelligence sources; the interception of communications; and the acquisition and disclosure of communications data is covered under the Regulation of Investigatory Powers Act 2000 (RIPA).

### 2 Principle 2 - compatible purposes

Personal data shall be obtained for only one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

### 3 Principle 3 - extent of data

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

### 4 Principle 4 - data accuracy

Personal data shall be accurate and, where necessary, kept up to date.

### 5 Principle 5 - retention period

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

## **6 Principle 6 - Data Subject Rights**

Personal data shall be processed in accordance with the rights of data subjects under this Act. Data subjects include service users, employees including temporary and volunteers and those communities we serve.

The rights that are applicable to all data subjects are:

- the right to be informed that processing is being undertaken;
- the right to access personal data;
- the right to prevent processing in certain circumstances;
- the right to rectify, block or erase data; and
- the right to claim compensation for certain breaches of the Act.

## **7 Principle 7 - security and management of data**

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss of, destruction of, or damage to personal data.

## **8 Principle 8 - foreign data transfer**

Personal data shall not be transferred to a country or territory outside the European Community unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

DRAFT

## PERSONAL INFORMATION

Personal information can be obtained from a number of sources, from the employee themselves, from the circumstances of their employment for example, salary information, from their progression through the organisation or from development, training and assessment situations.

This information then allows the organisation to plan and formulate policies and strategies and, in some instances, to conform to legislative requirements. Planning, policy and strategy formulation depends on information which is effective and accurate and will enable the organisation to recruit, train and develop employees to their full potential, to be as effective as possible within the organisation and to provide good service to our community.

It is the intention of the Service to hold information electronically where possible, in preference for paper based records.

Personal information on an employee must be held and maintained for a legitimate purpose which could include:

- as part of the recruitment process;
- to ensure a full and accurate account of the individual's employment history;
- to ensure payment of the correct level of salary, pension, and sick pay;
- to ensure that the proper levels of training are conducted for the specific role;
- to ensure emergency contact details are available;
- to provide the organisation with data from which management information can be obtained enabling policy and strategy formulation;
- to comply with legal obligations; and
- equality and diversity monitoring.

If information is withheld or not updated an employee may not receive benefits to which they are entitled.

### Personal Record File contents

#### Computerised Personal Record File

A computerised Personal Record File will hold the following information:

Type of information	Content	Purpose	Duration held
Employment	Original application form Employment references Qualification certificates Contract of employment (inc. relevant role profile)	Recruitment Recruitment Recruitment Recruitment	Minimum duration life of employment and 6 years after.

	<p>Next of kin information</p> <p>Details of promotion, and successful applications</p> <p>Transfers, successful requests and requests refused</p>	<p>Emergency contacts</p> <p>Career progression</p> <p>Equality and Diversity monitoring</p>	
Attendance	<p>Sickness record, PR25, Doctor's certificates</p> <p>Exemptions granted</p> <p>Correspondence issued under the Attendance Management Policy</p> <p>Copies of injury reports</p> <p>Attendance record cards</p> <p>Maternity leave applications</p> <p>Applications for special leave</p> <p>Parental leave applications</p> <p>Paternity leave applications</p> <p>Adoption leave applications</p> <p>PR12 Injury Report Forms</p>	<p>Sickness payments</p> <p>Management of attendance</p> <p>Maternity payments</p> <p>Management of attendance and appropriate payments</p> <p>Accident information</p>	<p>Minimum duration life of employment and 6 years after.</p>
Training	<p>Training courses nominations and results of attendance</p> <p>Examination results</p> <p>Application for post entry training</p> <p>Qualification certificates</p>	<p>Job competency and development</p> <p>Development</p> <p>Requirement of post entry training funding</p> <p>Development</p>	<p>Minimum duration life of employment and 6 years after.</p>
Performance	<p>Assessments/ advice/monitoring of performance</p> <p>IPDR form</p>	<p>Management of performance</p> <p>Personal development and</p>	<p>Minimum duration life of employment and 6 years after</p>



		review	
Awards/ Achievements	Compliments, Letters of thanks Achievements Letters of commendation	Personal achievement	Minimum duration life of employment and 6 years after
Discipline	Records of any disciplinary action taken, and associated papers where necessary	Management of discipline	Minimum duration life of employment and 6 years after
General Correspondence	General correspondence that does not fall within any of the categories above.	For example 'Request for reference'	Minimum duration life of employment and 6 years after

### Local Personal Record File

A Personal Record File maintained at the location of the individual must only contain the following items of information:

Section	Content	Purpose	Duration held
Training records	Permit to work	Job competency and development	Duration of employment
Performance	Assessments or warnings on performance  IPDR	Management of Performance  Personal development and review	Until end of warning of monitoring or improvement (then sent to PSS for PRF held for duration of employment)  Duration of employment
Attendance Management Information	Absence data	Monitoring	Duration of employment?

# APPENDIX 4

## ENVIRONMENTAL INFORMATION REGULATIONS 2004

### 1. PROCEDURES

The Environmental Information Regulations 2004 complement the Freedom of Information Act ([Standing Order 1/5](#)) and intend to provide a culture of openness and accountability amongst public sector bodies and enable the public to access information about any impact upon the environment of policies, processes and procedures.

In some ways, the Regulations are more encompassing than the Freedom of Information Act and many everyday requests for information may come under the definitions of the Environmental Information Regulations. Environmental Information is defined as information about:

- State of air, water, soil, land, landscape, natural sites.
- Substances, energy, noise, radiation, waste – and other releases into the environment.
- Policies, legislation, plans, etc. affecting above elements.
- Reports on implementation of environmental legislation.
- Economic analyses of environmental measures.
- Human health and safety, contamination of food chain.
- Effect of above elements on living conditions, cultural sites, built structures.

As many practices or events can impact upon the above elements the area covered by the Regulations is extensive.

#### 1.1 Rights of access/scope of regulations

Any person making a request for environmental information to a public authority is entitled to be informed in writing by the public authority whether it holds information of the description specified in the request and to have that information communicated.

This is commonly described as 'the duty to confirm or deny that information is held, and to provide it'.

The Environmental Information Regulations provide access in line with the Freedom of Information Act 2000 ([Standing Order 1/5](#)). There are, however, some differences which make the regulations more extensive.

The main differences are:

- The range of bodies covered by the EIR is wider to allow for consistency with the EC Directive and includes public utilities and certain public private partnerships and private companies, such as those in the water, waste, transport and energy sectors.
- Requests for environmental information need not be in writing.
- The information held by a public authority includes holding information held on behalf of any other person.
- The duty to provide advice and assistance requires a public authority to respond within 20 working days when requesting more particulars from the applicant.
- The time limits for responding to a request apply to ALL requests including those involving consideration of the public interest. Regulation 7 allows for an extension from 20 to 40 working days for complex and high volume requests.
- No exception is made for requests that will involve costs in excess of the 'appropriate limit' within the meaning of the Fees Regulations made under sections 9, 12 and 13 of the Freedom of Information Act. Except in specified limited circumstances, ALL requests must be dealt with and any charges imposed must be reasonable.
- There are differences in the exceptions available under Environmental Information Regulations and the exemptions available under Freedom of Information Act.
- The requirement for public authorities to have in place a complaints and reconsideration procedure to deal with representations alleging non-compliance with the Environmental Information Regulations is mandatory.

As the request does not have to be in writing, any verbal request for information of an environmental nature must be considered under the Regulations.

## **1.2 Requests for information**

Requests for information fall in line with the Freedom of Information Act 2000 but as requests can be verbal, it is important to document the name and correspondence address of the individual requesting the information, in order to reply to the request. (Email address is acceptable).

Some other features of requests for information are:

- The applicant does not have to mention the Regulations when making the request.
- An applicant has to identify him/herself for the purposes of the request, but the identity of the applicant is of no concern to the Authority except in the case of vexatious or repeated requests and personal information (see paragraph 3.4).
- The applicant need not be a United Kingdom national or resident. A request can be made by anybody, anywhere in the world.
- There is no restriction on the reasons why the information is being requested and the Authority cannot make enquiries as to why the information is being sought or what it will be used for.
- The Authority can request further information from the applicant in order to identify or locate the information.
- There are no formal requirements on applicants to describe the information in a certain way, for example, by reference number, but the description has to be sufficient to be able to locate and identify the information.

- The information communicated to the applicant has to be the information held at the time the request was received. Account may be taken of amendments or deletions that would have been made in the normal course of events.
- The Authority must help the applicant to frame a request for information if they are not able to do so themselves, for example writing down a request on the telephone and then confirming with the applicant the contents of the request are accurate.
- As soon as verification of the request is received the Authority has 20 working days to comply with the request (40 days for complex requests).

Each Authority can decide whether to charge for providing information that will satisfy the request, for example if there are substantial administration costs to gather and reproduce the information.

If a request for information is received in a department, section or on a station it must be forwarded immediately for the attention of the Data Manager, Data Management Section, marked 'Environmental Information Request'.

The Data Manager will be responsible for recording the request, obtaining the information from the relevant department, charging any appropriate fees and ensuring that the request is answered within the timescale.

The Data Manager will liaise with the Data Controller of the Section or Department concerned for assistance in providing the information requested. It is imperative that information is provided in a timely manner to ensure that the specified timescales are met.

### **1.2.1 Exceptions**

Under the Environmental Information Regulations there is a presumption of openness, irrespective of the date of the information unless an exception applies. There are two categories of exceptions:

- 3) Public interest – those in which the public authority seeking to reply on the exemption has to establish that the public interest in maintaining the exception outweighs the public interest in disclosing information.
- 4) Absolute – where no public interest test is required.

There are a number of exceptions to providing data under the Environmental Information Regulations. A public authority may refuse to disclose information to the extent that:

- It does not hold that information when an applicant's request is received.
- The request for information is manifestly unreasonable.
- The request for information is formulated in too general a manner and the public authority has complied with regulation 9 (that is, provided advice and assistance).
- The request relates to material which is still in the course of completion, to unfinished documents or to incomplete data; or
- The request involves the disclosure of internal communications.

Other circumstances which may provide an exemption consider whether disclosure of the information would adversely impact on:

- International relations, defence, national security or public safety.
- Course of justice.
- Intellectual property rights.
- Legal confidentiality of organisation's proceedings.
- Protection of legitimate economic interests.

- Information provided voluntarily but with no consent to its disclosure.
- Protection of the environment the information relates to.

The Data Manager will advise on the full range of exceptions if required and will consider whether an exception applies on receipt of a request for information under the Environmental Information Regulations.

DRAFT

# APPENDIX 5

## REUSE OF PUBLIC SECTOR INFORMATION REGULATIONS 2005

### 1. PROCEDURES

The Re-use of Public Sector Information Regulations 2005 were developed to promote the re-use of information as a valuable resource. The regulations therefore actively promote providing information created within the public sector, to be utilised for example by the private sector. The regulations allow public sector organisations to capitalise on information produced in the course of their duties, where perhaps it was previously felt improper to do so. The basic principles and objectives are:

- To identify public sector documents that are available for re-use.
- To make such documents available at marginal cost to the applicant.
- That public sector bodies deal with applications to re-use information in a timely manner which is open and transparent.
- The process should be fair, consistent and non-discriminatory.
- Best practice in providing the information is applied across the public sector.

#### 1.2 Scope of regulations

The regulations apply to all public sector bodies. To 're-use' means using a document for another purpose than it was initially made for. Although the regulations refer specifically to documents, 'document' means:

"...any content, including any part of such content, whether in writing or stored in electronic form or as a sound, visual or audio-visual recording, other than a computer program".

'Content' is defined as:

"...information recorded in any form".

#### 1.3 Requests for information

Requests for re-using information need to be dealt with in a similar manner to Freedom of Information requests and therefore need to be formally responded to by the Data Manager. If you receive a request, it is important to document the name and correspondence address of the individual requesting the information, in order to reply to the request (e-mail address is acceptable). In addition, the person making the request must specify the document requested and state the purpose for which the document is to be re-used.

The organisation is under no obligation to permit re-use of a document, but must respond to the request within 20 days. Once permission for re-use has been granted then certain conditions apply, such as:

- where available, the document is provided in an electronic format.
- there is no obligation to create or adapt a document for re-use.
- there is no obligation to continue to produce a document for re-use.

In addition, the organisation can impose conditions on re-use as long as these do not discriminate between applicants who request re-using a document for comparable purposes. The organisation cannot enter into an exclusive arrangement, or contract unless this would be in the public's interest, and then only after publishing the details of this arrangement.

## 1.4 Exemptions

The Regulations apply to all documents held by the Fire Service although the requirements of the Data Protection Act (see [Standing Order 2/16](#)) are not affected by the Regulations and therefore the processing of personal data must be fair: in general terms, this would require the explicit permission of an individual before their personal data is supplied in a document. In addition, there are exemptions to what can be supplied under the Regulations:

- Documents which would be exempt under the Freedom of Information Act
- Documents where the copyright or intellectual property rights belong to a person or organisation external to the Fire Service.
- Documents which fall out of the scope of the core tasks or responsibilities of the Fire Service.

Also for the regulations to apply, the document:

- Must have been identified as available for re-use.
- Must have been made available to the applicant, or has been provided by means other than through an application made under the Data Protection Act 1998, Freedom of Information Act 2000 or Environmental Information Regulations 2004

There are also public sector institutions which are exempt, such as Public Sector Broadcasters, Schools, Libraries and Museums.

## 1.5 Charging

The regulations allow for charging a fee for an applicant's re-use of an organisational document. This fee can be calculated to include the commercial value of re-use, that is to say the cost of collection, production, reproduction and dissemination, plus any return on investment. In practice, many documents such as digital documents would not cost very much to provide and may have little commercial value.

Any charges need to be reasonable and justifiable if audited. Under the regulations, it is not possible to charge one applicant to re-use a document and then allow another to re-use the same document in the same circumstances for free. The Regulations promote competition in the free market and therefore all applicants must be treated equally.

## 1.6 Partnerships

The Fire Service may enter into partnerships with other public and private sector organisations in the course of their operational activity. In general terms, it is important to nominate which public sector partner should have responsibility for authorising re-use: if both parties are public sector organisations, it is advisable to nominate one body to authorise the re-use of documents.

It should be made clear to any applicants that if any copyright or intellectual property rights belong to a private sector partner, then permission for re-use must be gained from that partner.

The Fire Service should not authorise a private sector organisation to authorise the re-use of public sector (Fire Service) documents.

## 1.7 Asset lists

In this context, an asset is a document which is of value to the organisation and therefore may be of value to others, if re-used. The organisation already maintains a list of types of information available under the Freedom of Information Act: this is called a publication schedule and will be added to with assets (documents) which may be re-used, indicating any charges which are payable if the documents are re-used. To enable efficient location of such documents, it is important that documents which are

being re-used are included on the publication schedule and that the Data Manager is informed of any documents which have the potential for re-use.

## **1.8 Important legislation to consider – classification of request**

The Re-use of Public Sector Information Regulations 2005 need to be considered in conjunction with the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. This set of legislation aims to encourage more open and accountable government by establishing a general statutory right of access to official records and information held by public authorities. These complement and are influenced by the Data Protection act 1998 as generally information which involves or can identify an individual is exempt.

Documents may be provided under the Freedom of Information Act free of charge, but the Re-use of Public Sector Information Regulations may allow for charges to be applied if the information is re-used. Therefore, any request for information needs to take into consideration the requirements of all three pieces of legislation. All requests of this nature must be forwarded to the Data Manager at Headquarters who will establish what legislation any request may come under, and provide a formal response.

DRAFT



# APPENDIX 6

## Requests for Information

