0105 Management of Information

ORDER NO. 1/5
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 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 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 is available to enable accurate classification of information assets.

The service will promote a culture of openness and accountability and where possible will publish information electronically on the service 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 organisation 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. For senior employees who are required to create SECRET or TOP SECRET documents, they should follow the handling instructions for these classifications.

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 2018

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 service will not understand what these labels mean
- 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 2**
- 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 2018).

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 and USB devices 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. The need to use removable electronic medium should be assessed as the strategy of the organisation is towards a cloud first mobile strategy and systems such as Microsoft Office 365 facilitate access to information in the cloud and reduce the need for portable removable media.

- 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
- 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 3 for further information about the Freedom of Information Act 2000.

The Data Protection Act 2018 gives data subjects the right to access personal information that the service 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 4 for further information about the Data Protection Act 2018.

Other legislation that may facilitate formal access to information is the Environmental Information Regulations 2004 (See Appendix 5) and the Re-use of Public Sector Information Regulations 2005 (See Appendix 6.

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 7 for Requests for Information Flowchart)

2.3 Data sharing

As part of collaborative arrangements with partner agencies, the service 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 service to target its resources in the most appropriate areas.

Information can only be shared with partner agencies when there is a sharing agreement in place. All sharing agreements must be created with the approval of the Data and Governance Manager and details of them must be stored by Data Management and CAD. All employees involved with this work must ensure they are aware of their roles and responsibilities under these agreements and are expected to operate within authorised procedures contained within them.

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 2.**
- 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 MESH 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 Electronic storage

Protectively marked material should be stored providing protection appropriate to the risk of compromise as follows:

- **OFFICIAL – WMFS PUBLIC, OFFICIAL- WMFS LOW, OFFICIAL – WMFS MEDIUM, OFFICIAL – WMFS HIGH:** Microsoft Office 365 has been approved by the Cabinet Office to store information up to and including OFFICIAL

2.4.3 Destruction of documents

- **OFFICIAL – WMFS PUBLIC**: no requirement to control disposal or destruction of documents
- **OFFICIAL- WMFS LOW:** all documents to be dispo*sed 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

2.4.4 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

2.4.5 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.

2.4.6 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.

2.4.7 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.

2.4.8 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

2.5 Telecommunications

2.5.1 Voicemail

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

2.5.2 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.**

2.5.3 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 talk group) 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.**

2.5.4 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**.

2.5.5 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 must not leave authority premises.

Permission to work at home or other non-service premises on protectively marked material up to and including OFFICIAL – WMFS MEDIUM is at the discretion of the employee's line manager. Caution and discretion must be used and it is the responsibility of the end user to protect the information.

2.6 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 other requests for information that have been received within the previous 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 service.

Any data protection breaches or security incidents will be monitored and reported to the SIRO and SET at the time of occurrence and periodically to provide a management view of potential risks to the organisation - **See Appendix 4, Data Protection Act 2018.**

3. BUSINESS AND SAFETY CRITICAL INFORMATION

Within the organisation there will be recognised communication channels to ensure that information that is operational safety and business critical is identified and appropriate processes exist to ensure that staff understand the content. The channels of communication are as follows:

3.1 Service News

News items relating to the Organisations events, activities, achievements, media related activity and other general items deemed appropriate by Corporate Communications. These must not to include any critical operational and/or business information relating to Corporate or Operational Risk or signposting to critical notices.

These must be approved by the Section Head or Department Manager through Corporate Communications

3.2 Routine Notice (RN)

This is for information that is general or routine operational and/or business information. These should not include any safety critical or business critical information relating to Corporate or Operational Risk or signposting to critical notices

These must be approved by the Section Head or Department Manager through the Document Processing Management (DPM) Section

3.3 Business Critical Notice (BCN)

These are critical messages related to the delivery of our services, systems and processes that may have a bearing on or impact Corporate Risk and where failure to carry out any necessary actions will affect the organisation's ability to carry out business functions.

I.e. Financial, reputational or affect the delivery of business related activities.

An assurance Mechanism will be introduced ensuring that end users receive, understand and/or complete any actions required because of this notice.

These must be approved by a Strategic Enabler through the Document Processing Management (DPM) Section or Incident Room Manager (out of hours during critical periods)

3.4 Safety Critical Notice (SCN)

These are critical health and safety messages and/or information relating to but not exclusively to operational staff. This is to communicate information directly related to the safety and welfare of personnel and to ensure the health, safety and welfare of staff when delivering core functions and services.

An assurance Mechanism will be implemented ensuring that end users receive, understand and/or complete any actions required because of this notice.

Failure to carry out any necessary actions could expose the communities of the West Midlands and personnel of West Midlands Fire Service to risk of serious injury or death.

These must be approved by Duty Area Commander through the Document Processing Management (DPM) Section or Incident Room Manager (out of hours during critical periods)

4. 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 2018.

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 adequately protected by encryption. Further information must be sought from ICT Service Desk if you are unsure whether your device is compliant.

5. CROSS REFERENCES

Information Commissioner's Office website

Local Government Transparency Code 2014

6. KEY CONSULTEES

Policy Team

All Strategic Enablers

FBU, UNISON, FOA

Data Management

SHE

7. PRIVACY IMPACT ASSESSMENT

A Privacy Impact Assessment (PIA) has been carried out and is available upon request from Data Management once approved by your section head

8. EQUALITY IMPACT ASSESSMENT

An Equality Impact Assessment has been carried out and is available upon request from Data Management once approved by your section head

9. OWNERSHIP

Strategic Enabler for ICT

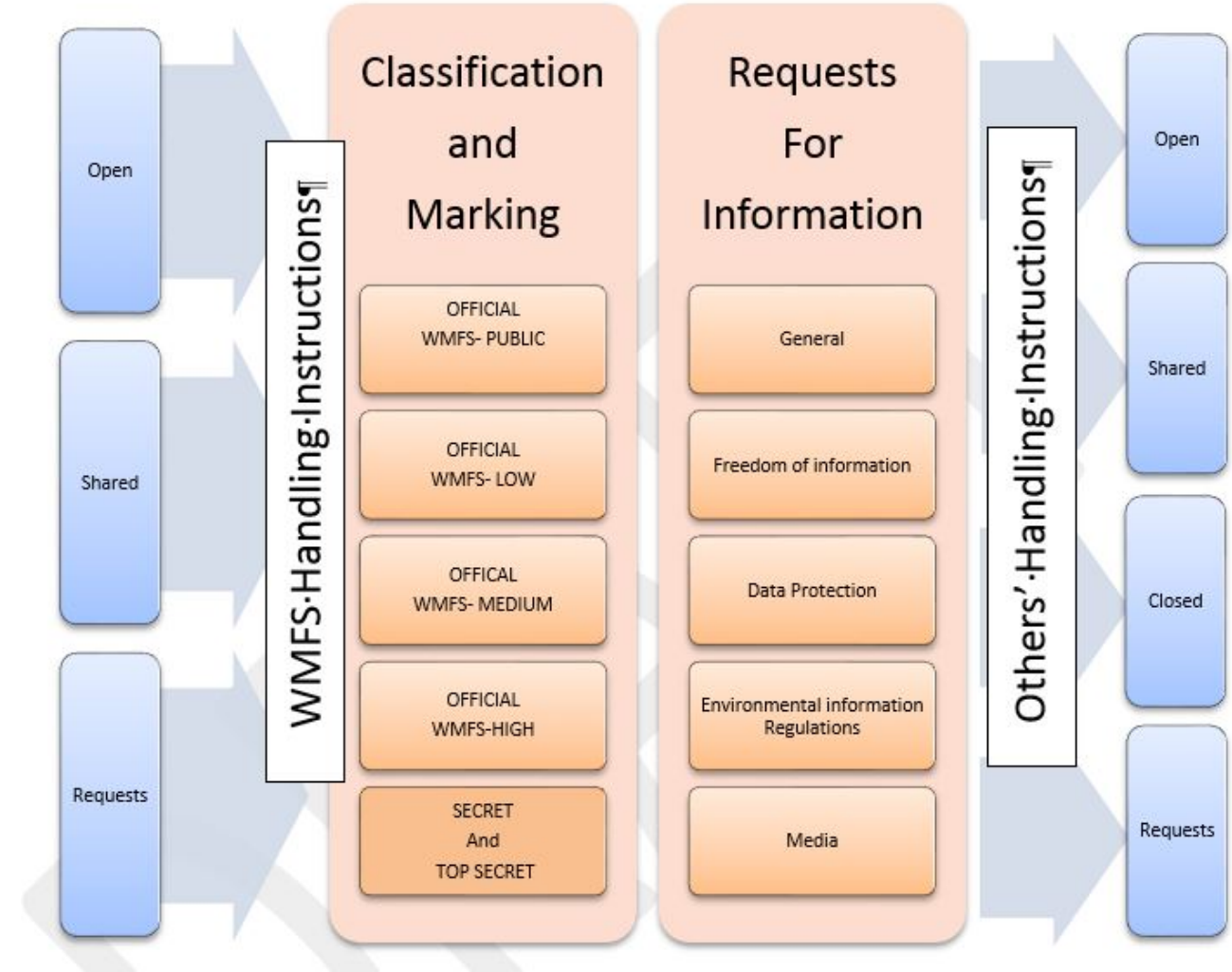
10. RESPONSIBILITY AND REVIEW

10.1 Created/Reviewed/Amended

This Order has been updated by the Data and Governance Manager in July 2018.

.

APPENDIX 1



APPENDIX 2
HANDLING INSTRUCTIONS

Protective Marking	Handling Instructions
OFFICIAL – WMFS PUBLIC	No controls or restrictions around the use of this information. It can be distributed freely Published on the internet. Accessed via personal devices with no restriction Transferred using removable media No requirement for secure disposal Unrestricted access to information Can be passed via pager Voicemail Mobile phone Airwave System ESN Fire ground radio
OFFICIAL – WMFS LOW	Documents must be stored behind single barrier e.g. Clear desk policy Suitable for posting through Royal mail Accessed via personal device Can be e-mailed from wmfs.net to less secure, personal network Can be stored on a personal device Can be passed via pager Documents disposed of in line with organizational policy Answerphones and Voicemail Mobile phone Airwave System ESN Fire ground radio
OFFICIAL - WMFS MEDIUM	Documents must be protected by two levels of

	protection e.g. (e.g. a locked container within a building with access controls) Suitable for posting through Royal mail Accessed via personal device with access protocols Documents must be shredded Can only be e-mailed from wmfs.net to wmfs.net or other secure network e.g. cjsm Cannot be stored on a personal device without encryption Cannot be passed via pager Disposal of electronic information must be managed by ICT Mobile phone Airwave System ESN
OFFICIAL – WMFS HIGH	Physical documents should be held in purpose built storage with restricted access Application data should be managed within a secure network No access to this information from personal devices Secure Clearance (SC) for regular access Must not be transferred using removable media Documents must be shredded Disposal of electronic information must be managed by ICT Can only be accessed from WMFS device Must only be e-mailed by wmfs.net to wmfs.net or secure network Not suitable for posting through Royal mail Mobile phone (caution should be exercised) Airwave System ESN

APPENDIX 3
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 service website and on MESH.

It is the responsibility of the Data and Governance 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.
- 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

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 and Governance Manager, Data Management section, marked 'Freedom of Information Request'.

The Data and Governance 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 and Governance 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 and Governance 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 and Governance 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 service 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.

In line with best practice, anonymised requests will be published in a Disclosure Log on the service website to further promote openness and transparency.

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 2018, 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 and Governance Manager at Headquarters who will establish what legislation any request may come under, and provide a formal response.

1.2.1 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 and Governance 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 2000.

APPENDIX 4
DATA PROTECTION ACT 2018

1. Procedures

West Midlands Fire Service fully endorse and adhere to the principles of the Data Protection Act 2018 which incorporates the European Union General Data Protection Regulations (EU GDPR).

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 Information Commissioner's Office is the data protection regulator and supervisory body for the United Kingdom. Its responsibility is to publish guidance and enforce compliance with the Ddata Protection Act 2018, Freedom of Information Act 2000, Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003.

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

Role Title	Position in the Organisation
Data Protection Officer	Data and Governance Manager
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 protect 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 2018 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 persnal data kept within their particular department to ensure that such data is maintained in accordance with the principles of the Data Protection Act 2018. 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
- Includes any intentions or opinions the Service may have towards the individual

Special Category data

The Data Protection Act 2018 defines special category 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
- Convictions, proceedings and criminal acts
- Genetics and biometrics

1.2 Employee 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.

1.2.1 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 2018.

Section 3.14.2 details the information that can be held in the Computerised Personal Record File.

1.2.2 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 2018.

A Personal Record File can be maintained at the location of the individual but must only contain the items of information as listed in Section 4.2

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.

1.3 Employee Access

1.3.1 Personal record file

All employees under the terms of the Data Protection Act 2018 are entitled to know what personal information the organisation holds about them and how it is being processed..

Every employee has the ability to view and print 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.

Requests to access personal information (including personal record files and occupational health files) that the organisation might hold should be made to the Data Protection Officer at Fire Service Headquarters. 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. The Data Protection Act 20181998 gives employees an entitlement to information and not documents

- If the employee wishes a third party to have access to their information, for example, a legal or trade union representative, this must be included in the request. Representatives will not be given access to and individual's personal file independently without the explicit written consent of the employee concerned.

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

1.4 Requests for information

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 30 days.

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 2018 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.

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.

1.4.1 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.

1.4.2 Requests for the 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.

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.

1.4.3 Requests and exchange of information with 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
- 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

1.5 Data Protection Breaches

It is important to understand if personal data is not handled correctly, there must be processes in place to contain and recover, assess the ongoing risk, notify appropriate parties of the breach and evaluate and respond to the data protection breach.

These are some examples of security incidents that may lead to the loss or compromise of personal data;

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorized use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

The above are examples of events that may lead to a data protection breach but if you are unsure then please seek further advice from the Data Protection Officer.

1.5.1 Data Protection Breach Process

If you are involved in an incident as defined in the examples above or determined by the Data Protection Officer as a data protection breach, then you must:

1. Contact the ICT Service Desk on 0121 380 6666 to record the event as a data protection breach.
2. The ICT Service Desk will liaise with the Data Protection Officer to determine the course of action to manage the incident.
3. The SIRO and relevant SET members will be notified of incident via an initial report.
4. The Data Protection Officer will manage the incident to conclusion and ensure that a log of the incident and all actions taken is maintained to identify trends or areas of weakness.
5. Post incident, an investigation will be instigated and the outcomes will be reported to the SIRO and members of SET.

   Management reports on data breaches will be sent out periodically to the SIRO and SET to ensure management are aware of potential risks to the authority.

2. Principles of the Data Protection Act 2018

There are 7 key principles under the Data Protection Act 2018

2.1 Principle 1 -processing should be lawful, fair and in a transparent manner fair processing

Personal data shall be processed fairly, lawfully and transparently, in particular, shall not be processed unless one condition of Article 6 of the EU GDPR is met:

Article 6 gives the following conditions for processing personal data:

- 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 Fire Services Act 2004);
- The processing is necessary to **protect the vital interests** of the data subject;
- The processing is necessary for tasks in the **public interest or the exercise of authority vested in WMFS**
- The processing is necessary for the purposes of **legitimate interests** pursued by WMFS

In the case of special category data, this includes; race, ethnic origin, political belief, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation, processing is permitted only where Article 6 conditions for processing personal data exists **and** a further condition specified in Article 9 of GDPR is met.

Article 9 gives the following conditions for processing personal data:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;

(c) processing is necessary to protect the vital interests of the data subject or of another where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to contract with a health professional;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;

It is difficult to envisage any activity which does not include processing and a Privacy Impact Assessment (PIA) should be completed when embarking on projects and/or activities that may involve processing personal data.

See Appendix 8

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).

See Appendix 9

2.2 Principle 2 - Collected for specified, explicit and legitimate purposes

Personal data should only be used for the purpose for which it was originally collected

2.3 Principle 3 – Data minimisation

The amount of personal data should be adequate, relevant and limited to what is necessary for the purpose it is held;

2.4 Principle 4 - Data accuracy

Personal data shall be accurate and kept up to date. Reasonable steps must be taken to ensure that any personal data that is inaccurate is erased or rectified without delay.

2.5 Principle 5 – Storage limitation

Personal data kept in a form where a data subject is identifiable shall not be kept for longer than is necessary for that purpose or purposes. Data that is out of date or no longer necessary must be properly destroyed or deleted.

2.6 Principle 6 – Technical and Organisational measures in the security and management of data

Personal data should be processed in a manner that ensures appropriate security. 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.

2.7 Principle 7 – Accountability

WMFS must be responsible for and be able to demonstrate compliance with the other 6 principles.

2.8 Employee 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.

3. Personal Record File contents

3.1 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)	ed	t Recruitment Recruitment Recruitment Emergency contacts		Minimum duration life of employment and 6 years after.

	Next of kin information Details of promotion, and successful applications Transfers, successful requests and requests refus		Career progression Equality and Diversity monitoring		
Attendance	Sickness record, PR25, Doctor's certificates Exemptions granted Correspondence issued under the Attendance Management Policy Copies of injury reports Attendance record c ards Maternity leave applications Applications for special leave Parental leave applications Paternity leave applications Adoption leave applications PR12 Injury Report Forms	Sickness payments Management of attendance Maternity payments Management of attendance and appropriate payments Accident information		Minimum duration life of employment and 6 years after.	

Training	Training courses nominations and results of attendance Examination results Application for post entry training Qualification certificates	Job competency and development Development Requirement of post entry training funding Development		Minimum duration life of employment and 6 years after.	
Performance	Assessments/ advice/monitoring of performance IPDR form	Management of performance Personal development and review	Minimum duration life of employment and 6 years after		
Awards/ Achie	vements	, 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 ye	ars after	
General Correspondence	General correspondence that does not fall	For example 'Request for reference'	Minimum duration life of employment		

	within any of the categories above.		and 6 years after	

3.2 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	Management of Performance	Until end of warning of monitoring or improvement (then sent to PSS for PRF held for duration of employment)
	IPDR	Personal development and review	Duration of employment
Attendance Management Information	Absence data	Monitoring	Duration of employment?

4. Data Subject Rights

Data subjects have the right to be informed about the collection and use of their personal data. Data subjects can be employees (including temporary and volunteers), partners and those communities we serve,

The rights that are applicable to all data subjects under DPA are as follows:

- Right to be informed that processing is being undertaken

This is achieved by issuing privacy notices at the point of collecting personal data

- Right to access personal data (requests)

There are processes in place to ensure requests are responded to promptly.

- Right to rectify, block or erase data

This is a limited right as some personal data has to be maintained in line with other legislation e.g. pension regulations so may not be erased on request

- Right to restrict processing of the data

This is a limited right as some personal data has to be processed in line with other legislation e.g. payment of council tax so cannot be restricted for this purpose

- Right to object to processing

This is a limited right as some personal data has to be processed in line with other legislation e.g. financial regulations to calculate taxation so objection cannot be acted upon in some instances

- Rights in relation to automated decision making including profiling

Processes have been identified within the organization and mechanisms put in place to verify the results and provide a simple explanation for the rationale behind the decision:

- Right to data portability

This gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller. This is applicable in situations such as entering into a contract such as changing banking providers but is not applicable to processing paper files;

- Right to claim compensation for certain breaches of the Act

APPENDIX 5
ENVIRONMENTAL INFORMATION REGULATIONS 2004

1. Procedures

The Environmental Information Regulations 2004 complement the Freedom of Information Act 2000 and enable the public to access information about any impact upon the environment of policies, processes and procedures.

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. 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 EU 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
- 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 and Governance ManagerData and Governance, Data Management Section, marked 'Environmental Information Request'.

The Data and Governance Manager Data and Governance 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.

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:

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 exception outweighs the public interest in disclosing information
2. 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
- 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 and Governance Manager Data and Governancwill 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.

APPENDIX 6
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.

1.1 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".

1.2 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 and Governance Manager, Data and Governance. 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.

1.3 Exemptions

The Regulations apply to all documents held by the Fire Service although the requirements of the Data Protection Act 2018 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 2000
- 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 2018, 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.

1.4 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.

1.5 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.

1.6 Asset lists

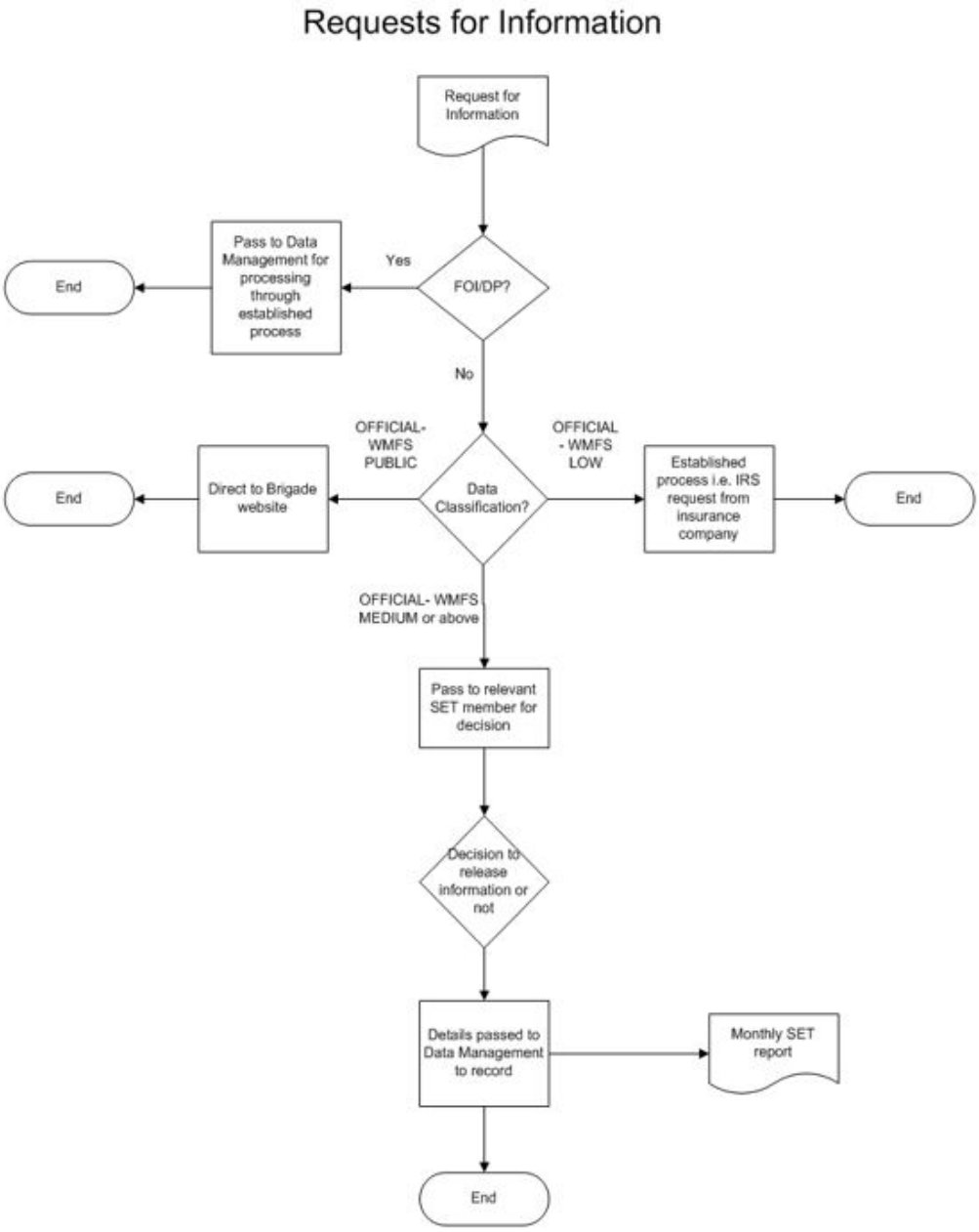
In this context, an asset is a document which is of value to the organisation and therefore may be of value to others, if re-used. The organisation already maintains a list of types of information available under the Freedom of Information Act: this is called a publication schedule and will be added 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 and Governance Manager is informed of any documents which have the potential for re-use.

1.7 Important legislation to consider – classification of request

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 and Governance Manager at Headquarters who will establish what legislation any request may come under, and provide a formal response.

APPENDIX 7



Appendix 8
PRIVACY IMPACT ASSESSMENTS (PIA)

1. Introduction

1.1 The Data Protection Act 2018 stipulates that privacy by design must be an integral part of information governance and PIAs are an essential part of this framework

1.2 PIAs are used as a systematic way to assess all policies, procedures, activities and proposed projects for impact on the privacy of employees of the West Midlands Fire Service and members of the public. It is a methodology of assessing the privacy risks associated with new projects or initiatives and what steps can be taken to mitigate the risk.

1.3 The methodology is issued by the Information Commissioner's Office, the overarching body for the regulation of data protection and associated areas. PIAs are intrinsically linked to data protection and provide some good practice surrounding the areas where an organisation may be vulnerable when processing personal data.

1.4 There are some aspects of data sharing that are governed by separate legislation which may also need to be considered during the PIA process, for example, Crime and Disorder Act 1998.

2. The Meaning of privacy

In its broadest term privacy is about the integrity of the individual. It therefore encompasses many aspects of the individual's social needs.

2.1 There are four aspects that are commonly used to assess the impact on privacy:-

2.1.1 The privacy of personal information:

individuals generally do not want data about themselves to be automatically available to other individuals and organisations.

2.1.2 The privacy of the person:

this is sometimes referred to as 'bodily privacy' and is concerned with the integrity of the individual's body, for example, compulsory immunisation or compulsory provision of samples of body fluid and tissue.

2.1.3 The privacy of personal behaviour:

this relates to the observation of what individuals do, and includes such issues as optical surveillance and 'media privacy', for example, CCTV.

2.1.4 The privacy of personal communications:

this relate to the freedom that individuals have to communicate amongst themselves, using various media, without routine monitoring of their communications by other persons or organisations.

Any new policy development, activity, service project or any policies being amended and reviewed must undergo a PIA. The aim of a PIA is to highlight the likely impact of the policy, activity or project on the four common aspects of privacy listed above and mitigate the privacy risk.

3. Privacy risks

A PIA is concerned primarily with minimising the risk of a data protection breach. Risk can arise through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long and insecurely

- disclosed to those who the person it is about does not want to have it;
- used in ways that are unacceptable to or unexpected by the person.

The assessment process requires policy leads to demonstrate that a number of key considerations surrounding privacy have been taken into account in developing or revising a policy or practice.

4. Benefits of a PIA

- The identification of the policy, activity or project's privacy impacts and the impact this will have;
- Building and demonstrating compliance to legislation;
- Reassurance to individuals that the WMFS is handling their information using best practice;
- A project which has been subject to a PIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way;
- Improve transparency and trust in the organisation
- Reduce the likelihood of the organisation failing to comply with legal obligations under the DPA as breaches of this legislation can lead to large fines from the ICO and loss of public trust.
- In the event of a Data Protection breach then we can show that as an organisation we have taken a considered approach to processing personal data and are committed to ensuring Privacy rights are upheld.
- Financial benefits as identifying potential issues at an early stage through a PIA will generally require a simpler and more cost-effective solution.
- Using PIAs will increase awareness of privacy and data protection issues

5. Projects that may require a PIA

A PIA should be carried out for all new projects, policies, procedures, activities and proposed projects within the organisation or if an existing project or initiative changes in any way that may impact a person's privacy.

Examples of when a PIA will need to be carried out:

· A new or upgraded electronic system for storing and accessing personal data;

· A data sharing initiative where two or more organisations seek to pool or link sets of personal data;

· A proposal to identify people in a particular group or demographic and initiate a course of action;

· Using existing data for a new and unexpected or more intrusive purpose;

· A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic Number Plate Recognition (ANPR) capabilities to existing CCTV).

· A new database which consolidates information held by separate parts of an organisation;

· Legislation, policy or strategies which will impact on privacy through the collection, use of information, through surveillance or other monitoring.

6. Responsibility for carrying out a PIA

The lead person on any policy formation, new project or review is responsible for making sure that PIA screening is undertaken and a full PIA is completed if required. This could be undertaken at the same time as an Equality Impact Assessment (EIA) as both assess impacts on people whether they are employees or service users.

The PIA template form is available on MESH`.

The Data Protection Officer and Governance Manager can provide advice guidance and assistance when requested but is not responsible for completing the PIA.

At the screening stage, members of staff responsible for completing PIAs will need to identify whether the policy, activity, function or project impacts directly on the privacy of employees or members of the public.

The PIA screening process involves answering a set of questions about the possible privacy impacts (risks) the project may have.

As a result of completing the PIA screening process then the outcome will be either 'Privacy risk level is low' or 'Privacy risk level is high'.

If the privacy risk is low then then reason for this will have to be justified within the screening process.

If the privacy risk is high then then a full PIA will need to be completed.

7. Conducting a PIA

The assessment process requires policy leads to demonstrate that a number of key considerations surrounding privacy have been taken into account in developing or revising a policy or practice.

The processes for conducting a PIA will include the following:

1. Identify the need for a PIA

2. Describe the information processing

3. Consultation process

Stakeholder groups - the various stakeholder groups may have different perspectives on these factors. If the screening is undertaken solely from the viewpoint of the organisation itself, it is likely that risks will be overlooked, therefore stakeholder perspectives should be considered as each question is answered.

4. Assess necessity and proportionality

5. Identify and assess risks

Use data you have gathered, or any previous data available to identify actual or potential impacts

6. Identify measures to reduce risks

7. Sign off and record outcomes

8. Monitoring

The PIA and the consultation on it, will have helped to anticipate its likely effects on the privacy of individuals or specific groups of people. Therefore, monitoring of the policy once it is in operation must be undertaken.

The final policy may be revised to take account of some or all of the privacy impact findings, but the actual impact of the policy will only be known once it is in operation.

9. Publication

All policy owners are responsible for ensuring that a full PIA is completed and sent electronically to the Data Management Section. A copy of the policy, new project details or review must also be attached to the PIA documentation. Details of all PIAs are available on request from Data Management.

APPENDIX 9

REGULATION OF INVESTIGATORY POWERS ACT 2000 POLICY FOR SURVEILLANCE, A COVERT HUMAN INTELLIGENCE SOURCES AND THE ACQUISITION OF COMMUNICATIONS DATA (See 2.4 of main order 2/16)

REGULATION OF INVESTIGATORY POWERS ACT 2000 POLICY FOR SURVEILLANCE, COVERT HUMAN INTELLIGENCE SOURCES AND THE ACQUISITION OF COMMUNICATIONS DATA

1. Introduction

1. The Regulation of Investigatory Powers Act 2000 (RIPA) provides a framework for control and supervision of investigatory powers exercised by public bodies, including local authorities, in order to balance the need to protect privacy of individuals with the need to protect others, particularly in light of the Human Rights Act 1998. RIPA provides a statutory basis for the authorisation and use by the security and intelligence agencies, law enforcement and other public authorities, of covert surveillance, agents, informants and undercover officers. It regulates the use of these techniques and safeguards the public from unnecessary invasions of their privacy.
2. RIPA covers the 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. RIPA also provides for the appointment of independent Surveillance Commissioners who will oversee the exercise by public authorities of their powers and duties.
3. Of conceivable relevance to the work of the Service are the provisions of Part ll of RIPA that cover the use and authorisation of 'directed' surveillance (section 28) and covert human intelligence sources (section 29) by public authorities. Part ll of RIPA provides for a new authorisation mechanism which authorities undertaking covert surveillance must use.
4. It may occasionally be necessary for officers to use covert surveillance techniques for the following reasons related to the core activities of the organisation:

- audit investigation;
- community safety;
- health and safety compliance;
- environmental protection and pollution control;
- potential fraudulent activities.

This list is not necessarily exhaustive.

1. This policy addresses solely issues having relevance to the activities of the Service and how the authorisation mechanisms required by the Act will be administered.
2. In addition, the investigatory powers will be exercised by the Service in compliance with the Codes of Practice contained in:-

- the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Code of Practice) Order 2002 (SI 2002/1932);
- the Regulation of Investigatory Powers (Covert Surveillance: Code of Practice) Order 2002 (SI 2002/1933); and
- the Regulation of Investigatory Powers (Communications Data) Order 2003: Home Office Draft Code of Practice entitled '*Accessing Communications Data*'.

2. The meaning of 'surveillance' within the Act

2.1 Covert 'directed' surveillance is covered by RIPA

Surveillance is 'directed' when it is undertaken in relation to a specific investigation or a specific operation which is likely to result in the obtaining of private information about a person.

Surveillance is covert where it is carried out in a manner calculated to ensure that the person or persons subject to the surveillance are unaware that it is or may be taking place.

Such forms of surveillance involve observing an individual or group of people whether through unaided observation or listening or through the use of technical devices and when information regarding their private or family lives is likely to be obtained.

2.2 Special provisions apply where information enjoying legal privilege or certain types of confidentiality may be obtained. In such circumstances, which are not expected to be relevant to the

Authority's activities, the approval of the Information Commissioner or the Authority's head of paid service is required.

3. The meaning of 'covert human intelligence sources' (CHIS) within the Act

1. When person A establishes, maintains or uses a relationship (personal or otherwise) with person B for information gathering purposes or uses, or discloses information obtained by such a relationship, or arising from it, and s/he does so when B is unaware that it is or may be happening, then person A is a Covert Human Intelligence Source.

4. the meaning of 'communications data' within the Act

1. Communications data is information held by communications service providers relating to communications made by their customers. This includes itemised call records, routing information and subscriber details. Communications data does not include the actual content of any communications.
2. The Service in acquiring this data must ensure that it is required either (1) in the interests of public safety, or (2) in preventing or detecting crime. Additionally, this information must be proportionate to what is sought to be achieved. In practical terms, this would cover such things as:-

- during a fire investigation, obtaining contact details in order to speak to whoever reported the fire to help piece together the sequence of events; or
- to investigate hoax or malicious calls.

1. It should be noted that the Act has no impact on the existing protocols relating to requests for data when responding to an emergency (999/112) call where the caller has cleared the line before giving adequate details about the location at which an attendance is required. These requests will continue to be dealt with under the Data Protection Act and in accordance with the procedures set out in the '*Code of Practice for the Public Emergency Call Services between Public Network Operators and the Emergency Services'.*

5. Authorisation - CHIS and 'directed' surveillance

1. The Service will apply a procedure for the proper authorisation and recording of its activities and for the use of CHIS in accordance with the Act.
2. The Service shall ensure that officers with responsibility for authorising the acquisition of communications data or carrying out surveillance and the use of CHIS shall be made aware of their obligations to comply with the Act and with this policy. Furthermore officers shall receive appropriate training or be appropriately supervised in order to carry out functions under the Act. In particular, all officers with responsibilities under the Act will be familiar with the Codes of Practice referred to above, so far as they relate to their responsibilities.
3. To ensure that these powers are used appropriately, authority for authorisation for surveillance or CHIS will be obtained from officers of the rank of Area Commander during office hours and outside hours from the Duty Principal Officer prior to commencement. Forms of Authorisation can be obtained from the Data and Governance Manager.

6. Review of authorisations and policy - CHIS and 'directed' surveillance

1. The Service will ensure that authorisations for surveillance or CHIS, once granted, are reviewed on a monthly basis and are renewed or cancelled as appropriate.
2. This policy and accompanying procedure shall be reviewed from time to time in light of changes in legislation, case law, or for the better performance of the procedure.
3. To provide an independent overview of Service activity, a half-yearly report will be provided to the Fire Authority by the Monitoring Officer. The information that will be given to the Fire Authority will be based on usage numbers only.

7. Procedure for surveillance - CHIS and 'directed' surveillance

1. When a member of the Service believes that it is necessary for surveillance ('directed' or CHIS) to be undertaken to enable the gathering of information, they should, in the first instance, discuss their request confidentially with the Data and Governance Manager. An Area Commander

(referred to as the Authorising Officer), or the Duty Principal Officer (also Area Commander level) will then authorise the request for surveillance to be undertaken.

2. Assuming that outline agreement is reached, then the officer initiating the request must complete and forward the form RIPA 1 'Application for the authorisation of 'directed' surveillance or RIPA 5 'Application for the authorisation of covert human intelligence source (CHIS)' to the Authorising Officer under private and confidential cover.
3. On receipt, the Authorising Officer will ensure that the application is provided with a reference number obtained from the Data and Governance Manager and that the details are recorded in the Service's RIPA database held by Data Management for entry onto the appropriate register file.
4. **Authorisations must only be granted for one month and then reviewed.**
5. The Authorising Officer will discuss the position with the officer making the original request, forwarding the appropriate forms for completion and return before the renewal date arrives.
6. Details of the completed forms and renewal date will be entered onto the Service's RIPA database by the Data Management team.
7. **Renewal of authorisations must only be granted twice.**
8. Surveillance can only be undertaken for a maximum of three months. If any further extensions of time are considered necessary, then the case must be discussed in detail with the Data and Governance Manager and the Strategic Enabler for People Support.

8. Report to Strategic Enabling Team

Every six months, the Data and Governance Manager is to provide the Strategic Enabling Team (SET) with details of any surveillance which has been authorised under this legislation.

The information that will be submitted to the Strategic Enabling Team will be details of usage numbers and reasons. No personal information will be released.