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.

Where it is possible that further information is needed before the request can be answered

An exemption applies

The public interest in maintaining the exemption outweighs the public interest in disclosing the information

When any fee is charged, and that fee is not paid within three months of fees notice being issued

If the public authority estimates the cost of complying with the request would exceed the 'appropriate limit'

If the request is vexatious or repeated

Under some exemptions, certain conditions must 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 must be met by anyone requesting information under the Act:

- Put it in writing
- Name and address of applicant (email address is acceptable)
- 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 must 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 must be enough 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 complement 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:

Public interest – those in which the public authority seeking to reply on the exemption must establish that the public interest in maintaining the exemption outweighs the public interest in disclosing information

Absolute – where no public interest test is required

There are several 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.

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 Data Protection Act 2018, Freedom of Information Act 2000, Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003.

The Service has defined several 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 personal data kept within their 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 into 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 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 can 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 organization 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 later.

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, 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 policy, 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 policy 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 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