WEST MIDLANDS FIRE AND RESCUE AUTHORITY

AUDIT AND RISK COMMITTEE

3 JUNE 2019

1. MONITORING POLICIES ON RAISING CONCERNS AT WORK – WHISTLE BLOWING STANDING ORDER 2/20 AND REGULATION OF INVESTIGATORY POWERS ACT 2000

Joint report of the Chief Fire Officer and the Monitoring Officer.

RECOMMENDED

1.1 THAT the Audit and Risk Committee notes that there have been no allegations of whistle blowing reported through the Whistle Blowing Policy (SO 2/20).

1.2 There have been no requests to enact the Regulation of Investigatory Powers Act 2000 in West Midlands Fire Service in the last year up to 31 March 2019.

1.3 THAT the Audit and Risk Committee notes the content of the Whistle Blowing Standing Order 2/20 (attached as Appendix 1) and the Management of Information Framework, Standing Order 1/5, Appendix 4, (attached as Appendix 2).

2. PURPOSE OF REPORT

2.1 There are no cases to report.

2.2 This report is submitted to inform the Committee of the monitoring of the referrals under the Whistle Blowing Standing Order 2/20 (attached as Appendix 1) and the use of the Regulation of Investigatory Powers Act under the Management of Information, Standing Order 1/5, Appendix 4, (attached as Appendix 2).

3. BACKGROUND

Whistle Blowing

3.1 Whistle Blowing Standing Order was consulted on 8th August 2018

with minor amendments and then published 6th December 2018.

3.2 In relation to Whistle Blowing; in May 1996 the Committee on Standards in Public Life stated that "All organisations face the risk of things going wrong or of unknowingly harbouring malpractice. Encouraging a culture of openness within an organisation will help: prevention is better than cure."

3.3 The Public Interest Disclosure Act 1998 sets out a framework for public interest whistle blowing which protects workers from reprisal because they have raised concern about malpractice. Only a disclosure that relates to one of the broad categories of malpractice can qualify for protection under the Act. These include concerns about actual or apprehended breaches of civil, criminal, regulatory or administrative law; miscarriages of justice; dangers to health, safety and the environment and the cover up of any such malpractice. Case law continues to develop this area of law.

3.4 In addition to employees, the Act covers for example, workers, contractors, trainees, agency staff. This list is not exhaustive.

3.5 To be protected, the person blowing the whistle must believe that their disclosure is "in the public interest", i.e. disclosure is made in the reasonable belief that there is an issue such as wrongdoing in public office or something that presents a risk to the public that warrants disclosure.

3.6 The Committee should note that there have been NO allegations of whistleblowing raised by an employee over the last twelve months using the Whistle Blowing Policy up to 31 March 2019.

3.7 **Data Protection**

Data Protection Framework sits as Appendix 4 within the Management of Information Standing Order 1/5 (attached as Appendix 2).

3.8 **Regulation of Investigatory Powers**

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.

3.9 The Committee should note that the Service has not approved any surveillance under RIPA legislation in the last twelve months up to 31 March 2019.

3.10 The West Midlands Fire Service will continue to raise awareness through training on the Whistle Blowing Policy, Management of Information and RIPA to all of our partners.

4. EQUALITY IMPACT ASSESSMENT

As part of the review and consultation process consideration is given to whether an IEIA is required, and therefore on this occasion this was not a requirement.

5. LEGAL IMPLICATIONS

5.1 Data Protection: depending on the level and or seriousness of a breach of the Data Protection Act 2018 and incoming Data Protection Bill 2018, there are various levels of prosecution ranging from enforcement notices, financial penalties and in extreme cases custodial sentences.

5.2 RIPA: if surveillance operations are not carried out in accordance with the safeguards as laid down in RIPA, the evidence obtained may not be admissible in legal proceedings and the Service may be subject of a claim on infringing the human rights of the person under surveillance.

6. FINANCIAL IMPLICATIONS

There are no direct financial implications arising from this report.

7. ENVIRONMENTAL IMPLICATIONS

There are no environmental implications arising from this report.

BACKGROUND PAPERS

The Public Interest Disclosure Act 1998 (PIDA)

The contact name for this report is Phil Hales, Deputy Chief Fire Officer, telephone number 0121 380 6907.

PHIL LOACH
CHIEF FIRE OFFICER

SATINDER SAHOTA
MONITORING OFFICER TO THE AUTHORITY

Appendix 1

WEST MIDLANDS FIRE SERVICE

02/20 WHISTLE BLOWING POLICY

Overview of Amendments

1 STRATEGY

Following the Public Interest Disclosure Act (PIDA), which came into force in July 1999 (updated on 1st May 2013 GOV.UK), legal protection is now provided to employees who raise concerns about suspected dangerous or illegal activity that they are aware of through their work. The common term for voicing such concerns is 'whistle blowing'. West Midlands Fire Service (WMFS) wishes to create an open and honest culture with its statutory obligations, detailed in the Act, and ethical standards, detailed in its Core Values. Details on our core values can be found in the Equality & Diversity Policy

2 PURPOSE

The Public Interest Disclosure Act 1998 makes sure that employees, contractors providing services, most agency workers, home workers and trainees on vocational and work experience schemes are legally protected in raising concerns responsibly.
External contractors may encounter wrongdoing that affects WMFS. Therefore, this whistle blowing policy is also open to employees of our contractors.
Whistle blowing is when an employee reports suspected wrongdoing at work. Officially this is called 'making a disclosure in the public interest'

3 RESPONSIBILITIES

3.1 Employee Responsibilities

A whistle blower is an employee, you! You report certain types of wrongdoing. This will usually be something you've seen at work - though not always.

The wrongdoing you disclose must be in the public interest. This means it must affect others, e.g. the general public.

As a whistle blower you're protected by law - you shouldn't be treated unfairly or lose your job because you 'blow the whistle'.

You can raise your concern at any time about an incident that happened in the past, is happening now, or you believe will happen in the near future.

Employees are often the first to realise that there may be something seriously wrong with the organisation that employs them. They may be able to alert the organisation early on to things like fraud, negligence, bribery and health and safety risks. However, they may not express their concerns, because they feel that speaking up would be disloyal to their colleagues or to the organisation. They may also fear harassment or victimisation. In these circumstances they may feel it easier to ignore the concern rather than report what may be no more than a suspicion of malpractice.

The procedures in this order give ways for individuals to raise concerns and receive feedback on any action taken. It makes sure that individuals receive a response and know how to pursue concerns if they are not happy with the response. It gives reassurance that individuals will be protected from possible reprisals or victimisation if they believe they have made a disclosure.

You're protected by law if you report any of the following:

- a criminal offence, eg fraud
- someone's health and safety is in danger

- risk or actual damage to the environment
- a miscarriage of justice
- the company is breaking the law, eg doesn't have the right insurance
- you believe someone is covering up wrongdoing

Complaints that don't count as whistleblowing

Personal grievances (eg bullying, harassment, discrimination) aren't covered by whistleblowing law, unless your particular case is in the public interest. Report these under our Grievance Policy 2/2

3.2 Management Responsibilities

The action taken by the Service will depend on the nature of the concern. The matters raised may be investigated internally by an appropriately experienced officer knowledgeable in the area concerned, for example, audit, Line Manager or HR Practitioner.

Alternatively, through the disciplinary process, the matter may be referred to the police, the external auditor or may be the subject of an independent enquiry.

In order to protect individuals and the Service, and those accused of misdeeds or possible malpractice, initial enquiries will be made to decide whether an investigation is appropriate and, if so, what form it should take. Concerns or allegations that fall within the scope of specific procedures, for example, unfair discrimination issues, will normally be referred for consideration under those procedures. Some concerns may be resolved by agreed action without the need for investigation. Members of the SET can seek guidance from the Strategic Enabler - People at any stage in the investigation.

Within 10 working days of a concern being raised, the individual with whom the concern was raised will write to the complainant:

- acknowledging that the concern has been received;
- indicating how the matter is to be dealt with;
- giving an estimate of how long it will take to provide a final response;
- telling the complainant whether any initial enquiries have been made;
- supplying the complainant with information on staff support mechanisms; and
- telling the complainant whether further investigations will take place and if not why not.

The amount of contact between the officer(s) considering the issues will depend on the nature of the matters raised, the potential difficulties involved and the clarity of the information provided. If necessary, further information will be sought from the complainant in a discreet manner.

When any meeting is arranged, the complainant will have the right to be accompanied by a representative body or a work colleague. The meeting can be held off site if requested.

West Midlands Fire Service will take steps to minimise any difficulties, which may be experienced as a result of raising a concern and provide any appropriate support. For instance, if required to give evidence in disciplinary or criminal proceedings, the Service will advise the complainant of the procedure and give reasonable support. Subject to legal constraints, complainant will receive information about the outcomes of investigations.

Upon completion of the investigation, all documents will be forwarded to the Strategic Enabler People.

3.3 Responsible Officer

The Strategic Enabler - People has overall responsibility for the maintenance and operation of this policy. This officer maintains a record of concerns raised and the outcomes (but in a form which does not endanger the complainant's confidentiality) and will report as necessary to the Service and Fire Authority.

4 PROCEDURES

4.1 How to raise a concern

If the matter relates to any fraudulent or corrupt activity, concerns should be raised in accordance with procedures detailed in the 0122 Anti-Fraud Corruption and Bribery Policy.

If the complainant wishes to raise or discuss any issues which might fall into the above category then the complainant should contact a member of Strategic Enabling Team (SET), the Treasurer or the Clerk to the Fire Authority, who will be required by WMFS to treat the matter in confidence.

Where possible, the complainant should raise their complaint in writing setting out the background and history of the concern giving names, dates and places where possible and the reason why the complainant is particularly concerned about the situation. If the complainant does not feel able to put the concern in writing, then the complainant can discuss the concerns verbally with a member of the SET, or the Treasurer/ 151 Officer or the Clerk to the Fire Authority.

The earlier that the complainant can express the concern and the more detail that can be provided, the easier it will be for the Service to take appropriate and necessary action. Remember:

- the complainant must disclose the information
- the complainant must believe it to be substantially true
- the complainant must not act maliciously or make false allegations
- the complainant must not seek any personal gain

At this stage the complainant will not be expected to prove the allegation, but will need to demonstrate to the person contacted that there are sufficient grounds for reasonable suspicion or concern.

The complainant may invite a member of the trade union representative body or a work colleague to be present during any meetings or interviews in connection with the concerns raised.

Where a concern relates to a Brigade Manager or SET Manager, then either the Strategic Enabler People (as Responsible Officer), or Deputy Chief Fire Officer or Chief Fire Officer, as appropriate, should be contacted in the first instance. Satinder Sahota as the Monitoring Officer role for the Fire Authority. The Monitoring Officer may be contacted via email Satinder.sahota@wmfs.net.

The Treasurer to the Fire Authority may be contacted on 0121 380 6919. The Clerk to the Fire Authority may contacted on 0121 380 6678. Address for the Treasurer and the Clerk to the Fire Authority is: West Midlands Fire Service, 99 Vauxhall Road, Birmingham, B7 4HW.

4.2 Confidentiality

All concerns will be treated in confidence and every effort will be made not to reveal the identity of the complainant. However, it is likely that further investigation will be necessary and the complainant maybe required to attend a disciplinary or investigative hearing as a witness at the appropriate time. An employee raises a concern confidentially if they give their name only on condition that it is not revealed without their consent. A concern is raised anonymously if the employee does not give their name.

4.3 Harassment or Victimisation

West Midlands Fire Service recognises that the decision to report a concern can be a difficult one to make, not least because of the fear of reprisal from those responsible for the alleged malpractice. The Service will not tolerate harassment or victimisation and will take action to protect the complainant when a concern is raised.

4.4 Untrue Allegations

If the complainant makes an allegation, but it is not confirmed by the investigation, no action will be taken against the complainant. If however the complainant makes an allegation which, upon full investigation, is found to have been malicious or vexatious, disciplinary action will be considered and the protection of the PIDA will be lost.

4.5 Anonymous Allegations

This policy encourages the complainant to put their name to the concerns. Concerns expressed anonymously are much less powerful, but will be considered at the discretion of the Strategic Enabler - People.

In exercising this discretion the factors to be taken into account would include the:

- seriousness of the issues raised;
- credibility of the concern; and
- likelihood of confirming the allegation from attributable sources and information provided.

4.6 How the matter can be taken further

This policy is intended to provide the complainant with an avenue to raise concerns within the Service. We hope the complainant will be satisfied with the response. If not, the complainant must indicate this to the Strategic Enabler - People or the Treasurer or Clerk or Monitoring Officer to the Fire Authority.

Legal advice may be sought on any concerns about malpractice. If the employee feels it is right to take the matter outside the Service, the following are possible contacts:

- The complainant's recognised trade union
- Citizens Advice Bureau
- A solicitor
- The Police
- Relevant professional bodies or regulatory organisations, such as Ombudsmen.

Public Concern at Work (www.pcaw.co.uk) is a charity that offers free advice to people concerned about danger or malpractice in the workplace, but who are unsure whether, or how, to raise the matter.

5 CROSS REFERENCES

This Policy makes reference to and complements issues contained in other Policies, namely:

0122 Anti-Fraud Corruption and Bribery Policy

0201 Disciplinary Procedure

0217 Dignity at Work

6 KEY CONSULTEES

Minor changes only have been made to this Order and consultation was not necessary.

7 EQUALITY IMPACT ASSESSMENTS

The initial Equality Impact Assessment raised no issues so a full impact assessment was not required.

8 OWNERSHIP

This Policy did not require Authority or SET approval.

9 RESPONSIBILITY AND REVIEW/AMENDMENT DETAILS

9.1 Responsible Strategic Enabler Team Member/Department

Strategic Enabler People/People Support Services

9.2 Created/fully reviewed/amended

This Policy has been reviewed, amended by People Support Service July 2018

Appendix 2

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 unauthorized 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)		Recruitment Recruitment Recruitment Emergency contacts Career		Minimum duration life of employment and 6 years after.

	Next of kin information Details of promotion, and successful applications Transfers, successful requests and requests refused		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 cards 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/ Achievements		Letters of thanks Achievements Letters of commendation	Personal achievement	Minimum duration life of employment and 6 years after	
Discipline	Records of any disciplinary action taken, and associated papers where necessary	Management of discipline	Minimum duration life of employment and 6 years after		
General Correspondence	General correspondence that does not fall within any of the categories above.	For example 'Request for reference'	Minimum duration life of employment and 6 years after		

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

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