WEST MIDLANDS FIRE AND RESCUE AUTHORITY

AUDIT COMMITTEE

4 JUNE 2018

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 Committee notes that there has been no allegation 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 2018.

1.3 THAT the Audit 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

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 The Whistle Blowing Standing Order was consulted on 4th June 2014 and then published 27th November 2014. Minor amendments

were made to include names of new personnel who have responsibilities under Whistle Blowing.

This Standing Order is currently under review and will be published by August 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 has been no allegations of whistleblowing raised by an employee over the last twelve months using the Whistle Blowing Policy up to 31 March 2018.

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 2018.

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

In preparing this report an Equality Impact Assessment is not required, due to the fact that all our policies have Equality Impact Assessments carried out when updating and amending.

5. LEGAL IMPLICATIONS

5.1 Data Protection: depending on the level and or seriousness of a breach of the Data Protection Act 1998 and incoming Data Protection Bill 2017, 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

Monetary Penalty notices: fines of up to £500,000 under current Data Protection Act 1998 but rising to 4% of turnover or income circa Euro 20m for serious breaches under the incoming European Union General Data Protection Regulations that are in force from 25th May 2018.

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

ORDER 2/20
WEST MIDLANDS FIRE SERVICE WHISTLE BLOWING POLICY

1 STRATEGY

Following the Public Interest Disclosure Act 1998 (PIDA), which came into force in July 1999, 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 by being compliant 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 Standing Order 0213 or 'The Plan':

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 it may be 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.

2 PROCEDURE

2.1 What the policy covers

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.

The subject of concern may be something unlawful, against the Service's policies, below established standards of practice, or that amounts to improper conduct. The overriding concern should be that it would be in the public interest for the alleged malpractice to be corrected.

Whistle blowing is when an employee reports suspected wrongdoing at work. Officially this is called 'making a disclosure in the public interest'.

An employee can report things that aren't right, are illegal or if anyone at work is neglecting their duties, including:

- Someone's health and safety is in danger
- Damage to the environment

- A criminal offence
- The company isn't obeying the law (like not having the right insurance)
- Covering up wrongdoing
- Behaviours that are being displayed

Distinction between grievance and whistle blowing

Whistle blowing occurs when an employee raises a concern about danger or illegality that affects others, not themselves personally. When someone raises a concern through the Service's grievance procedure, they are saying that they have personally been poorly treated and they are seeking redress or justice for themselves. The whistle blowing policy is intended to cover concerns that fall outside the scope of grievance or other existing Service procedures.

2.2 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 the 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 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 for People (as Responsible Officer), or Deputy Chief Fire Officer or Chief Fire Officer, as appropriate, should be contacted in the first instance. The Assistant Chief Executive, Melanie Dudley at Sandwell MBC has the Monitoring Officer role for the Fire Authority. The Monitoring Officer may be contacted on 0121 569 3513. Address: Sandwell Council House, PO Box 2374, Oldbury, West Midlands, B69 3DE.

The Treasurer to the Fire Authority may be contacted on 0121 3806919. 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.

2.3 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.

2.4 How the Service will respond

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 of 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 of People.

2.5 Responsible Officer

The Strategic Enabler of 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.

2.6 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.

2.7 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.

2.8 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 of 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.

2.9 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 of 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.

3 CROSS REFERENCES

This Standing Order makes reference to and complements issues contained in other Orders, namely:

0122 Anti-Fraud Corruption and Bribery Policy

0201 Disciplinary Procedure

0217 Dignity at Work

4 KEY CONSULTEES

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

5 EQUALITY AND DIVERSITY

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

6 OWNERSHIP

This Standing Order did not require Authority or SET approval.

7 RESPONSIBILITY AND REVIEW/AMENDMENT

7.1 Responsible SET Member/Department

Strategic Enabler People/HR Employee Relations Team

7.2 Created/fully reviewed/amended

This Standing Order has been reviewed, amended by Employee Relations in November 2014 and amended in October 2015.

Appendix 2

APPENDIX 4
DATA PROTECTION ACT 1998

1. PROCEDURES

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

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

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

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

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

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

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

1.1 Scope of personal data

Definition of Personal data or information
Is any information held electronically (including all emails) or manually – which relates to a ***living*** individual who can be identified:

- From the information

- From the information combined with other information which is in the possession of the Service or is likely to come in to the possession of the Service
- Includes any intentions or opinions the Service may have towards the individual

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

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

(See Appendices 1 and 2 for further information)

1.2 Personal records

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

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

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

1.2.1 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 1998.

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

1.3 Local Personal Record File

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

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

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

All information must be kept securely and in confidence.

1.4 Employee Access

1.4.1 Personal record file

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

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

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

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

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

1.4.2 Occupational health records

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

1.4.3 Other personal records

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

1.5 Information released to a third party

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

1.5.1 Sports and Welfare

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

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

1.6 Requests for information

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

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

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

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

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

1.6.1 Requests for incident information

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

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

All such requests must be submitted in writing by the party wishing to obtain the information. This is to be forwarded to the Central Administration team at e-mail

address InformationDisclosure@wmfs.net. A fee will usually be charged for this information.

1.6.2 Release of information for legal proceedings

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

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

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

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

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

1.6.3 Definition of documents (legal proceedings)

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

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

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

1.6.4 Information received or requested from the police about employees

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

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

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

1.7 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 Manager.

1.7.1 Data Protection Breach Process

If you are involved in an incident as defined in the examples above or determined by the Data Manager 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 Manager 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 Manager 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. Schedule 2 Conditions (Data Protection Act 1998)

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

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

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

3. Schedule 3 Conditions (Data Protection Act 1998)

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

- The data is of sensitive personal nature consisting of information as to racial or ethnic origin
- The individual has given their explicit consent to the processing
- The processing is necessary for the purposes of exercising or performing any right conferred or obligation imposed by law on the Data Controller in connection with employment
- The processing is necessary to protect the vital interests of the individual in a case where either the consent cannot be given (incapacity, for example) or else the Data Controller cannot reasonably be expected to obtain consent (for example, the individual cannot be contacted despite various attempts over a considerable length of time)
- The processing is carried out in the course of its legitimate activities by anybody or association not established for profit and which exists for political, philosophical or trade union purposes, and which relates only to individuals who are members of that body
- The individual has already made the information public, by taking deliberate steps
- The processing is necessary for the purpose of or in connection with legal proceedings, obtaining legal advice or establishing or exercising or defending legal rights
- The processing is necessary for the administration of justice or exercise of crown functions
- The processing is necessary for medical purposes and is undertaken by a health professional
- The personal data are processed in circumstances specified in an order made by the Secretary of State.

Information Commissioner's Office

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

4. Principles of the Data Protection Act 1998

4.1 Principle 1 - fair processing

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

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

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

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

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

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

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

4.1.1 Principle 2 - compatible purposes

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

4.1.2 Principle 3 - extent of data

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

4.1.3 Principle 4 - data accuracy

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

4.1.4 Principle 5 - retention period

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

4.1.5 Principle 6 - Data Subject Rights

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

The rights that are applicable to all data subjects are:

- Right to be informed that processing is being undertaken

- Right to access personal data
- Right to prevent processing in certain circumstances
- Right to rectify, block or erase data
- Right to claim compensation for certain breaches of the Act

4.1.6 Principle 7 - security and management of data

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

4.1.7 Principle 8 - foreign data transfer

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

4.2 PERSONAL INFORMATION

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

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

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

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

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

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

Personal Record File contents

Computerised Personal Record File

A computerised Personal Record File will hold the following information:

Type of information	Content	Purpose		Duration held
Employment	Original application form Employment references Qualification certificates Contract of employment (inc. relevant role profile) Next of kin information Details of promotion, and successful applications Transfers, successful requests and requests refused	Recruitment Recruitment Recruitment Recruitment Emergency contacts Career progression Equality and Diversity monitoring		Minimum duration life of employment and 6 years after.
Attendance	Sickness record, PR25, Doctor's certificates Exemptions granted Correspondence issued under the Attendance Management Policy	Sickness payments Management of attendance Maternity		Minimum duration life of employment and 6 years after.

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

Local Personal Record File

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

Section	Content	Purpose	Duration held
Training records	Permit to work	Job competency and development	Duration of employment
Performance	Assessments or warnings on performance	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?