WEST MIDLANDS FIRE SERVICE
DATA PROTECTION ACT 1998

1. STRATEGY

That the West Midlands Fire and Rescue Authority (hereinafter to be known as the Authority) and the West Midlands Fire Service (hereinafter to be known as the Service) fully endorse and adhere to the principles of the Data Protection Act 1998.

The Authority regards the lawful and correct treatment of personal information as very important to successful operations, and to maintain confidence between service users, employees including temporary and volunteers and those communities we serve. The Authority 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 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.

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

Data Protection Officer	Data Management Officer
Internal Data Controller	Senior member of staff 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.

2. PROCEDURES

The Data Protection Officer has responsibility to co-ordinate the Authority'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. This role has been assigned to the post of Data Management Officer.

Planning and reviewing the Service's Data Protection Policy, Strategy and Procedures will be carried out by the Data Management Officer on a regular basis, not less than annually.

Each department and fire station will have a designated representative(s) to act as a point of liaison with the Data Management Officer.

The Data Controller will also monitor personal data kept at their particular station or department to ensure that such data is maintained in accordance with the principles of the Data Protection Act. However, this does not absolve individuals from their responsibility of ensuring that personal data is maintained in accordance with the principles detailed in 2.2 below.

An employee wishing to know personal data about themselves should contact Human Resources as per Standing Order 2/21 Personal Information Policy.

2.1 Scope of personal data

2.1.1 Personal data or information

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

2.1.2 Sensitive data

Staff have to be aware that the processing of sensitive information is limited to a small number of specified purposes, for example, the provision of health information to managers by the Occupational Health Centre to re-integrate long term sickness absentees back into the workplace.

The Data Protection Act defines sensitive data as;

- the racial or ethnic origin of the data subject;
- their political opinions;
- their religious beliefs or other beliefs of a similar nature;
- whether they are a member of a trade union;
- their physical or mental health condition;
- their sexual life; and
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

However, the Service does not keep or process all of this data, only that which it legitimately needs to or has obtained with the approval of a data subject.

For further specific guidance, see Standing Order 2/21, Personal Information Policy.

2.2 Principles of the Data Protection Act 1998

2.2.1 Principle 1 - fair processing

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

Schedules 2 and 3 are attached – Appendix 1

If you do not meet at least one criterion, you 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 in **Schedule 2** is met; and
- in the case of sensitive personal data (defined in 2.1.2), at least one of the conditions in **Schedule 3** 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.

The PIA process is attached - Appendix 2.

If an organisation or individual holds any data that matches any of the above criteria, then they will have to legitimise why they are holding this data. An organisation or individual 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).

The RIPA process is attached - Appendix 3.

2.2.2 Principle 2 - compatible purposes

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

2.2.3 Principle 3 - extent of data

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

2.2.4 Principle 4 - data accuracy

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

2.2.5 Principle 5 - retention period

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes. Some guidance about retention timescales exists in Standing Order 2/21 Personal Information Policy.

2.2.6 Principle 6 - data subject rights

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

The rights that are applicable to all data subjects are:

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

2.2.7 Principle 7 - security and management of data

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

2.2.8 Principle 8 - foreign data transfer

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

2.3 Access to information

The Data Protection Act 1998 confers a right of access for data subjects to both computerised and manual data. This right of access depends on the way the data is kept, as access is available to 'structured filing systems'. The Act defines a relevant filing system as:

> 'Any set of information relating to individuals to the extent that, although the information is not structured by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a way that particular information relating to a particular individual is readily accessible'. For example, Personal Record Files would be regarded as a 'structured filing system'.

Advances in technology have also impacted on how the Service processes personal information. E-mails are commonly used to transfer information about individuals **BUT** the same eight principles listed above are applicable, that is, the data subject has the right to know that information is being processed about them and also rights of access see 2.2.6 Principle 6.

The Data Protection Act requires that an organisation registers with the Information Commissioner's Office the types of information held about individuals, the reason for holding such information, and the circumstances in which that information will be used.

Certain personal information is recorded for Government purposes. However, the justification of recording identification details of living individuals should be established on every occasion.

The Service will notify the Information Commissioner of the purpose and processing details of this procedure.

2.3.1 Unincorporated clubs or associations

(Station Social Clubs, Sports and Welfare Associations and Benevolent Fund).

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.

2.4 Requests for information

Departments or stations will have a nominated data controller. All requests for information in whatever form, for example, paper records, computer records, tapes, and so on, should be forwarded through the Internal Data Controller who will then liaise with the Data Management 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 Management Officer, Data Management Section, marked 'Data Protection Request'. If possible, the information should be sent by e-mail.

The Data Management 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 the Employee Relations team within the Human Resources Department.

The Data Management Officer will liaise with the data controller of the section, 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.

2.4.1 Requests for incident information

The Service is constantly receiving 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 FDR1 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 Data Management section in the Resources Directorate. Where necessary, Data Management will obtain the authority of the data subject before agreeing to any request for information.

A fee will usually be charged for this information.

2.4.2 Release of information for legal proceedings

When the Fire Authority 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.

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.

A request for such documentation will usually be made by the Litigation Section to the relevant section, department or station. A thorough search must be made for all relevant documents.

All such documents, upon request, will be forwarded, as soon as practically possible, to the Litigation Section.

This request includes **all** relevant documents, including original or rough notes, and whether they are supportive or potentially damaging.

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

In certain circumstances, it may be necessary to forward original documents held. On such occasions, the requesting officer will determine whether new documentation is to be commenced, or whether original documents will be returned.

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.

2.4.3 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 FDR1 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 discloseable 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.

2.4.4 Requests for information from fire safety departments

Requests in respect of fire safety advice or information will be directed to the data controller of the nearest fire safety centre or Fire Safety Section of the Technical and Operational Support Directorate for action.

2.4.5 Information received or requested from the police about employees

On occasions, the Service has been 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. Discussions with the police have indicated that 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;
- given that all employees are obliged to notify the Service if they have been charged with a criminal offence, senior officers should no longer 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;
- personnel who are being questioned or detained by the Police and who would be unable to report for duty as a result, should request the police to contact Fire Control and inform the duty officer that they will be unable to attend for duty. The duty principal command officer will then be informed and will take appropriate action; and
- requests from the police for copies of tapes from Fire Control will be managed and actioned by Fire Control. The procedure is detailed in Fire Control.

2.5 Complaints

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

2.6 Important legislation to consider

The Freedom of Information Act 2000 (see Standing Order 1/5) and the Environmental Information Regulations 2004 (see Standing Order 1/10) enable individuals to request access to information held by the Service. 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 compliments and is influenced by the Data Protection Act 1998, as generally information which involves, or can identify an individual is exempt; however, there may be requests for information, which will only in part identify an individual. Similarly, a request may refer to individuals, but in the majority may relate to information held which can be provided. Therefore, any request for information needs to take into consideration the requirements of all three pieces of legislation. All requests of this nature must be

forwarded to the Data Management Officer at Fire Service Headquarters who will establish what legislation any request may come under, and provide a formal response.

2.7 Further information

Further information or clarifications can be obtained from the Data Management Officer, telephone number 0121 380 6535.

3. CROSS REFERENCES

Standing Order 1/5 – Freedom of Information Act 2000

Standing Order 1/10 – Environmental Information Regulations 2004

Standing Order 1/17 – Re-use of Public Sector Information Regulations 2005

Standing Order 2/21 – Personal Information Policy

Standing Order 21/1 – Customer Care and Compliments, Comments and Complaints (CCC Policies)

4. KEY CONSULTEES

Operations Commander Birmingham North

Station Commander Woodgate Valley

Station Commander Bournbrook

Station Commander Canley

Station Commander Bickenhill

Station Commander Solihull

Ladywood Red Watch

Walsall White Watch

Handsworth Green Watch

Coventry Blue Watch

Brierley Hill Purple Watch

Human Resources Employee Relations Manager

Group Commander B FiReControl and Firelink Project

Equality and Diversity

Integrated Risk Management Team

Safety, Health and Environmental Team

Fire Brigades' Union

Fire Officers' Association

UNISON

Chief's Policy Advisor

Word Processing Unit

5. EQUALITY IMPACT ASSESSMENT

6. OWNERSHIP

The preliminary impact assessment screening raised issues which were dealt with by a full impact assessment.

This Standing Order did not require Corporate Board or Authority approval.

7. RESPONSIBILITY AND REVIEW / AMENDMENT

7.1 Responsible Corporate Board Member / Department

Director, Resources/Data Management.

7.2 Created / fully reviewed / amended

This Order has been reviewed by the Data Management Officer in January 2011 and Appendix 2 has been inserted by HR Employee Relations in November 2011.

Reviewed and amended November 2012.

Reviewed and amended May 2013.

APPENDIX 1

1. Schedule 2 Conditions (Data Protection Act 1998)

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

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

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

2. Schedule 3 Conditions (Data Protection Act 1998)

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

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

- the processing is necessary for the administration of justice or exercise of crown functions;
- the processing is necessary for medical purposes and is undertaken by a health professional; or
- the personal data are processed in circumstances specified in an order made by the Secretary of State.

APPENDIX 2

PRIVACY IMPACT ASSESSMENTS (PIA)

1. Introduction

1.1 PIAs are used as a systematic way to assess all policies, procedures, activities and proposed projects for impact on the privacy of employees of the West Midlands Fire Service and members of the public. PIAs are similar to Equality Impact Assessments (EIA) and there is not a legislative requirement to undertake them within the Fire and Rescue Service but they are mandatory within central government. It is a suggested methodology of assessing the privacy risks associated with new projects or initiatives and what steps can be taken to mitigate the risk.

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

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

1.4 There are no consequences for not undertaking PIAs but if a data breach occurs and the methodology is not used, then the likelihood is that greater fines and harsher enforcement action could be taken against the organisation.

2. The meaning of privacy

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

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

2.1.1 The privacy of personal information:

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

2.1.2 The privacy of the person:

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

2.1.3 The privacy of personal behaviour:

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

2.1.4 The privacy of personal communications:

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

Any new policy development, activity, service project or any policies being amended and reviewed should undergo a PIA. The aim of a PIA is to highlight the likely impact of the policy, activity or project on the four common aspects of privacy listed above. It will also determine the extent of any differential impact and identify ways in which the policy should be changed or this impact mitigated if adverse.

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

3. Reasons for undertaking a PIA

- Identifying and managing risks
- Avoiding unnecessary costs
- Inadequate solutions
- Avoiding loss of trust and reputation
- Informing the organisation's communication strategy

4. The outcomes of a successful PIA

The outcomes of an effective PIA are:

- the identification of the policy, activity or project's privacy impacts;
- appreciation of those impacts from the perspectives of all stakeholders;
- an understanding of the acceptability of the project and its features by the organisations and people that will be affected by it;
- identification and assessment of less privacy-invasive alternatives;
- identification of ways in which negative impacts on privacy can be avoided;
- identification of ways to lessen negative impacts on privacy;
- where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them; and
- documentation and publication of the outcomes.

5. Purpose

If the policy, project, activity has a significant impact on the privacy of people then a full **PIA must be completed.**

A full PIA is **not** likely to be required when:

- there are no concerns of adverse impact but a data compliance check should be undertaken to ensure compliance with the Data Protection Act 1998

A small-scale PIA is **likely to be** required when:

- there may be some concern or evidence of negative or adverse impact. An example of this is the application of existing personal data to a new purpose

A full PIA **will be** required when:

- there is substantial concern or evidence of negative or adverse impact. An example of this would be compulsory substance testing for all employees.

6. Who is responsible for carrying out PIAs?

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

The person responsible for completing the PIA has the responsibility to make sure that the Data Management Officer is provided with **electronic copies** of the full PIA in addition to maintaining a file of the original documentation and supporting evidence.

The Data Management Officer can provide advice guidance and assistance when requested.

7. Initial PIA screening process

At the screening stage, members of staff responsible for completing PIAs will need to identify whether the policy, activity, function or project impacts directly on the privacy of employees or members of the public and make an informed and clearly justifiable decision based on the analysis of data as to whether an activity requires a PIA and if so whether it is a small-scale or full PIA.

PIAs are one way in which an organisation can design privacy into its policy and procedures and meet their obligations under the Data Protection Act 1998 and the Human Rights Act 2000. Proportionality is a key principle and the scale of the PIA should reflect this.

The following aspects should be considered.

Scope and timescales for project or activity (including review date)

Detail how long this policy, activity or project is expected to run or how long it will take to implement. Also state the expected time scale when you expect to review the activity and any impacts on privacy.

Outline of main aims of this activity, policy or project

Be specific, what are the intended outcomes of your activity? How do you plan to achieve them?

Who will benefit or be affected by this policy or activity?

Will your activity affect staff and/or service users? Who is it intended to benefit? Who could it affect? It is not enough to put that it will affect all service users.

(a) Service users and community?

Will the activity affect different groups differently? Do you have any data on this if it is an existing strategy? Consider direct impacts and less obvious indirect impact. What are the demographics of the service users it will affect? If you do not have any data you cannot make an informed decision which you may later have to justify. If you have little data and a differential impact is likely or possible then you should consider a full or small-scale PIA.

(b) WMFS employees?

How many staff could it affect, both directly and indirectly? Do you have data on the make up of the staff affected. (Will it affect job roles? Working locations?)

Requirement for PIA and level required

This section must include the decision about the PIA requirement and justification as to whether the outcome is 'PIA not required'. 'Small-scale PIA' or 'Full PIA'.

You must justify your decision as to whether a full PIA is needed or not, consider:

- proportionality;
- the actual or potential impact; and
- data you have gathered, or any previous data available.

The completed initial PIA is then sent to the Data Management team who will review and get back to you within 12 working days

8. Conducting a PIA

Once the level of PIA has been determined, the process for completing a PIA for any project needs to reflect the nature of the project (for example, new system, replacement system, enhancements to an existing system, new technology, outsourcing, changed business processes or staff instructions, replacement user interface, revised privacy policy statement, drafting of legislative changes).

There are 5 suggested phases and these need not be formalised.

- preliminary phase;
- preparation phase;
- consultation and analysis phase(s);
- documentation phase; and
- review and audit phase.

8.1 Preliminary phase

The preliminary phase should have as deliverables, a project outline, a preliminary assessment of privacy concerns and some preliminary talks with key stakeholders.

8.2 Preparation phase

In this phase, organisations may undertake a stakeholder analysis, development of a consultation strategy and plan. Due to the nature of a small-scale PIA, these tasks do not need to be formalised.

8.3 Consultation and analysis phase(s)

This includes consultations with stakeholders, risk analysis, the articulation of problems and the search for constructive solutions.

Consultation does not have to be a formal process and can be limited to the stakeholders who have a key interest in the project or those who may have the biggest concerns about the project.

The key deliverable is a document (such as a privacy design features paper or a meeting outcomes report) that details the privacy impacts identified and the solutions or actions which will be taken to deal with them.

8.4 Documentation phase

The purpose of the documentation phase is to document the process and the outcomes. The deliverable is a PIA Report, which may draw heavily on the document produced during the consultation and analysis phase. Depending on the context, this might be a relatively brief 'note to file', with copies to relevant parties; but circumstances may justify a more carefully prepared document.

8.5 Review and audit phase

The purpose of this phase is to ensure that the design features arising from the PIA are implemented and are effective. The deliverable is a review or update report. Once again, in some contexts a 'note to file', with copies distributed to relevant parties, might be sufficient to achieve this requirement. In other cases, a more detailed document may be required.

9. Monitoring

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

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

10. Publication

All policy owners are responsible for ensuring that a full PIA is completed and sent **electronically** to the Data Management Section. A copy of the policy must also be attached to the PIA documentation.

The full reports will be made available on the Data Management intranet site and brief summary reports published on the WMFS internet site. The full reports will also be made readily available to anyone who requests a copy and arrangements will be made

to provide the results of PIAs in alternative languages and alternative formats as and when requested.

Criteria for small-scale PIA

This section provides guidance for evaluating whether a small-scale PIA should be conducted.

The evaluation depends on sufficient information about the policy, activity or project having been collected when preparing for the PIA screening process. The evaluation process involves answering a set of questions about characteristics of the project or the system that the project will deliver.

The 15 questions about project characteristics

Technology

(1) Does the project involve new or inherently privacy-invasive technologies?

Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.

Justification

(2) Is the justification for the new data-handling unclear or unpublished?

Individuals are generally much more accepting of measures, even measures that are somewhat privacy-intrusive, if they can see that the loss of privacy is balanced by some other benefits to themselves or society as a whole.

Identity

An identifier enables an organisation to collate data about an individual and identifiers are used for multiple purposes to enable data consolidation. Increasingly onerous registration processes and document production requirements imposed are warning signs of potential privacy risks.

(3) Does the project involve an additional use of an existing identifier?

(4) Does the project involve use of a new identifier for multiple purposes?

(5) Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous?

Data

(6) Will the project result in the handling of a significant amount of new data about each person, or significant change in existing data-holdings?

(7) Will the project result in the handling of new data about a significant number of people, or a significant change in the population coverage?

(8) Does the project involve new linkage of personal data with data in other collections, or significant change in data linkages?

The degree of concern about a policy, activity or project is higher where data is transferred out of its original context. The term 'linkage' encompasses many kinds of activities, such as the transfer of data, the consolidation of data-holdings, the storage, amalgamation and matching of personal data from multiple sources.

Data handling

(9) Does the project involve new or changed data collection policies or practices that may be unclear or intrusive?

(10) Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory?

(11) Does the project involve new or changed data security arrangements that may be unclear or unsatisfactory?

(12) Does the project involve new or changed data access or disclosure arrangements that may be unclear or permissive?

(13) Does the project involve new or changed data retention arrangements that may be unclear or extensive?

(14) Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?

Exemptions

(15) Will the project give rise to new or changed data-handling that is in any way exempt from legislative privacy protections?

Perspectives to consider

As with the criteria for full-scale PIA, risks may be overlooked unless these questions are considered from the various perspectives of each of the stakeholder groups, rather than just from the viewpoint of the deaprtment or section that is conducting the policy, activity or project.

Applying the criteria

Where the answers to questions are "Yes", consideration should be given to the extent of the privacy impact and the resulting risk to the policy, activity or project. The greater the significance, the more likely that a small-scale PIA is warranted.

Full PIA assessment guidance notes

Step 1 – Criteria for full-scale PIA

This section provides guidance for evaluating whether a full-scale PIA should be conducted. The evaluation depends on sufficient information about the policy, activity or project having been collected during the previous step.

The evaluation process involves answering the following set of 11 questions about key characteristics of the project and the system that the project will deliver.

The answers to the questions need to be considered as a whole, in order to decide whether the overall impact and the related risk, warrant investment in a full-scale PIA.

The 11 questions about key characteristics of the policy, activity or project

Technology

(1) Does the policy, activity or project apply new or additional information technologies that have substantial potential for privacy intrusion?

Examples include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.

Identity

(2) Does the project involve creating new ways to identify people, for example, identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?

Examples of relevant policy, activity or project features include a digital signature initiative, a multi-purpose identifier, interviews and the presentation of identity documents as part of a registration scheme and an intrusive identifier such as biometrics.

(3) Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?

Many functions cannot be effectively performed without access to the individual's identity and some others do not require identity. An important aspect of privacy protection is sustaining the right to interact with organisations without declaring one's identity.

Multiple organisations

(4) Does the project involve multiple organisations, whether they are government agencies (for exampe, in 'joined-up government' initiatives) or private sector organisations (for example, as outsourced service providers or as 'business partners')?

Schemes of this nature often involve the breakdown of personal data silos and identity silos and may raise questions about how to comply with data protection legislation. This breakdown may be desirable for fraud detection and prevention and in some cases for business process efficiency. However, data silos and identity silos have in many cases provided effective privacy protection.

Data

(5) Does the policy, activity or project involve new or significantly changed handling of personal data that is of particular concern to individuals?

The Data Protection Act identifies a number of categories of 'sensitive personal data' that require special care. These include racial and ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life, offences and court proceedings.

There are other categories of personal data that may give rise to concerns, including financial data, particular data about vulnerable individuals, and data which can enable identity theft.

Further important examples apply in particular circumstances. The addresses and phone-numbers of a small proportion of the population need to be suppressed, at least at particular times in their lives, because such **'persons at risk'** may suffer physical harm if they are found.

(6) Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?

Examples include intensive data processing such as welfare administration, healthcare, consumer credit, and consumer marketing based on intensive profiles.

(7) Does the policy, activity or project involve new or significantly changed handling of personal data about a large number of individuals?

Any data processing of this nature is attractive to organisations and individuals seeking to locate people, or to build or enhance profiles of them.

(8) Does the policy, activity or project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?

This is an especially important factor. Issues arise in relation to data quality, the diverse meanings of superficially similar data-items, and the retention of data beyond the very short term.

Exemptions and exceptions

(9) Does the policy, activity or project relate to data processing which is in any way exempt from legislative privacy protections?

Examples include law enforcement and national security information systems.

(10) Does the policy, activity or project's justification include significant contributions to public security measures?

Measures to address concerns about critical infrastructure and the physical safety of the population usually have a substantial impact on privacy. This may result in tensions with privacy interests, and create the risk of opposition and non-adoption of the programme or scheme.

(11) Does the policy, activity or project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?

Disclosure may arise through various mechanisms such as sale, exchange, unprotected publication in hard-copy or electronically-accessible form, or outsourcing of aspects of the data-handling to sub-contractors.

Third parties may not be subject to comparable privacy regulation because they are not subject to the provisions of the Data Protection Act or other relevant statutory provisions

Perspectives to consider

It is important to appreciate that the various stakeholder groups may have different perspectives on these factors. If the analysis is undertaken solely from the viewpoint of the organisation itself, it is likely that risks will be overlooked. It is therefore recommended that stakeholder perspectives are also considered as each question is answered.

Applying the criteria

Once each of the 11 questions has been answered individually, the set of answers needs to be considered as a whole, in order to reach a conclusion as to whether a full-scale PIA is warranted. If it is, a conclusion is also needed as to whether the scope of the PIA should be wide-ranging, or focused on particular aspects of the policy, activity or project.

APPENDIX 3

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

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

1. Introduction

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) provides a framework for control and supervision of investigatory powers exercised by public bodies, including local authorities, in order to balance the need to protect privacy of individuals with the need to protect others, particularly in light of the Human Rights Act 1998. RIPA provides a statutory basis for the authorisation and use by the security and intelligence agencies, law enforcement and other public authorities, of covert surveillance, agents, informants and undercover officers. It regulates the use of these techniques and safeguards the public from unnecessary invasions of their privacy.

1.2 RIPA covers the carrying out of 'directed' and intrusive covert surveillance; the use of covert human intelligence sources; the interception of communications; and the acquisition and disclosure of communications data. RIPA also provides for the appointment of independent Surveillance Commissioners who will oversee the exercise by public authorities of their powers and duties.

1.3 Of conceivable relevance to the work of the Service are the provisions of Part ll of RIPA that cover the use and authorisation of 'directed' surveillance (section 28) and covert human intelligence sources (section 29) by public authorities. Part ll of RIPA provides for a new authorisation mechanism which authorities undertaking covert surveillance must use.

1.4 It may occasionally be necessary for officers to use covert surveillance techniques for the following reasons:

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

This list is not necessarily exhaustive.

1.5 This policy addresses solely issues having relevance to the activities of the Service and how the authorisation mechanisms required by the Act will be administered.

1.6 In addition, the investigatory powers will be exercised by the Service in compliance with the Codes of Practice contained in:-

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

2. The meaning of 'surveillance' within the Act

2.1 Covert 'directed' surveillance is covered by RIPA.

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

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

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

2.2 Special provisions apply where information enjoying legal privilege or certain types of confidentiality may be obtained. In such circumstances, which are not expected to be relevant to the Authority's activities, the approval of the Information Commissioner or the Authority's head of paid service is required.

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

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

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

4.1 Communications data is information held by communications service providers relating to communications made by their customers. This includes itemised call records, routing information and subscriber details. Communications data does not include the actual content of any communications.

4.2 The Service in acquiring this data must ensure that it is required either (1) in the interests of public safety, or (2) in preventing or detecting crime. Additionally, this information must be proportionate to what is sought to be achieved. In practical terms, this would cover such things as:-

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

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

5. Authorisation - CHIS and 'directed' surveillance

5.1 The Service will apply a procedure for the proper authorisation and recording of its activities and for the use of CHIS in accordance with the Act.

5.2 The Service shall ensure that officers with responsibility for authorising the acquisition of communications data or carrying out surveillance and the use of CHIS shall be made aware of their obligations to comply with the Act and with this policy. Furthermore officers shall receive appropriate training or be appropriately supervised in order to carry out functions under the Act. In particular, all officers with responsibilities under the Act will be familiar with the Codes of Practice referred to above, so far as they relate to their responsibilities.

5.3 To ensure that these powers are used appropriately, authority for authorisation for surveillance or CHIS will be obtained from the Director of Human Resources or, if not available, the Duty Principal Officer prior to commencement. Forms of Authorisation can be obtained from the Litigation Officer.

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

6.1 The Service will ensure that authorisations for surveillance or CHIS, once granted, are reviewed on a monthly basis and are renewed or cancelled as appropriate.

6.2 This policy and accompanying procedure shall be reviewed from time to time in light of changes in legislation, case law, or for the better performance of the procedure.

6.3 To provide an independent overview of Service activity, a half-yearly report will be provided to the Fire Authority by the Monitoring Officer. The information that will be given to the Fire Authority will be based on usage numbers only.

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

7.1 When a member of the Service believes that it is necessary for surveillance ('directed' or CHIS) to be undertaken to enable the gathering of information, they should, in the first instance, discuss their request confidentially with the Litigation Officer. The Director of Human Resources, (referred to as the Authorising Officer), or, in his absence, the Duty Principal Officer will then authorise the request for surveillance to be undertaken.

7.2 Assuming that outline agreement is reached, then the officer initiating the request must complete and forward the form RIPA 1 'Application for the authorisation of 'directed' surveillance or RIPA 5 'Application for the authorisation of covert human intelligence source (CHIS)' to the Authorising Officer under private and confidential cover.

7.3 On receipt, the Authorising Officer will ensure that the application is provided with a reference number obtained from the Human Resources database and that the details are typed onto the Service's RIPA database held by the Human Resources Department for entry onto the appropriate register file.

7.4 **Authorisations must only be granted for one month and then reviewed.**

7.5 The Authorising Officer will discuss the position with the officer making the original request, forwarding the appropriate forms for completion and return before the renewal date arrives.

7.6 Details of the completed forms and renewal date will be entered onto the Service's RIPA database by the Human Resources Department.

7.7 **Renewal of authorisations must only be granted twice.**

7.8 Surveillance can only be undertaken for a maximum of three months. If any further extensions of time are considered necessary, then the case must be discussed in detail with the Litigation Advisor or the Director of Human Resources.

8. Report to Corporate Board

Every six months, the litigation advisor is to provide Corporate Board with details of any surveillance which has been authorised under this legislation.

The information that will be submitted to Corporate Board will be details of usage numbers and reasons. No personal information will be released.