

SO/11/1 - Data Protection in HFRS

Target Audience: WT RT NU

Owner: Information Compliance Officer

Author: Service Information Compliance Officer

Contact: Service Information Compliance Officer

Amended date: 12/2012

Next review due: 12/2013

1 Policy

1.1 Hampshire Fire and Rescue Authority (HFRA) are required to notify the Information Commissioner, before any processing commences of Hampshire Fire and Rescue Service (HFRS) data within a relevant filing system, of the following:

1.1.1 The nominated Information Compliance Officer.

Publicised detail (Notification) of the personal data being or to be processed including:

- The category of data subject to which they relate (e.g. employees, relatives, healthcare);
- A description of the purpose or purposes for which the data is being or will be processed;
- A description of any recipient to whom the data may be disclosed;
- Those countries outside the EEA to which any data is to be transferred; and
- A general description of the security measures to be taken to comply with the Seventh Data Protection Principle.

1.2 The 'Notification' must be reviewed annually with the Information Commissioners Office.

1.3 A copy of the 'Notification' is available from the Information Compliance Officer and can also be viewed on the Information Commissioner's website at [Information Commissioners Office - notification register](#) (type Hampshire Fire and Rescue Service in the name field).

1.4 The Hampshire Fire and Rescue Authority (Data Controller) and its senior management fully endorse and adhere to the Principles of the Data Protection Act 1998 (DPA).

1.5 The HFRA regards the lawful and correct treatment of personal information (Data Processing) as very important to successful operations, and to maintain confidence between service users, employees and those it serves. The HFRA guarantees that the Service will treat personal information lawfully and correctly.

1.6 An individual (Data Subject), whose information is either held or processed by HFRS has the right to access the material held, and to be assured that it will only be processed in accordance with the Eight Principles of the Data Protection Act 1988. (Appendix A).

1.7 HFRS has the right to make a charge (currently £10.00) for subject access requests.

1.8 The designated role of the Information Compliance Officer is to co-ordinate the Authority's response to the Act, and to ensure that the provisions of the Act are met.

1.9 The Information Compliance Officer is the first point of contact on any of the issues mentioned in this policy document.

1.10 The Information Compliance Officer will be responsible for dealing with all internal and external enquiries.

1.11 The CCTV systems are operated in line with the Information Commissioners Data Protection CCTV Code of Practice 2008. (To be read in conjunction with Appendix B -CCTV [SO/11/5](#)).

- The Information Compliance Officer has overall responsibility for the compliance of the system and has a legal requirement to ensure all employees work to the CCTV Surveillance Code of Practice.
- Day to day observance of the CCTV system is the responsibility of the appointed person as identified in the CCTV [SO/11/5](#).

1.12 Planning, reviewing, and developing the Service's Data Protection strategy will be carried out by nominated members of the Service Performance Review Team, on a regular basis.

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

1.14 A continuous programme of awareness training will be provided to existing and new employees including seminars and the provision of literature.

1.15 Where personal data needs to be passed outside the Service it will in general be done with the Data Subject's consent except where this is not possible or where required by law (Data Protection Act Exemptions such as crime prevention/detection, prevention of injuries, or where it is in the person's vital interests.)

1.16 Any employee breaching the requirements of the Act may be subject to both internal disciplinary procedures and legal action under the DPA.

All staff are personally liable and upon conviction can be liable to a fine of up to £500,000. Offences include:

- Notification related – failure to notify or acting outside notification;
- Failure to comply with written requests for particulars;
- Unlawful obtaining or disclosure of personal data;
- Knowingly or recklessly, without the consent of the Data Controller, to obtain or disclose personal data.

2 Fair processing notice

2.1 The Hampshire Fire and Rescue Service [fair processing notice](#) may be found on our intranet and internet. When collecting personal information from an individual they must be made aware of the services fair processing notice. Queries on fair processing notices should be directed at the Information Compliance Officer.

3 Procedures

3.1 Collection of personal data

3.1.1 Personal data means information held about living individuals. It may be on computer systems or as manual records and includes all personal data relating to you.

3.1.2 To ensure that the receipt of information into HFRS databases is consistent and accurate, and the information is identified, validated, processed and disposed of in accordance with the DPA the following procedures must be used:

- The Service Information Compliance Officer must be advised of all personal data processing within HFRS by submitting an [FM/11/1/11](#).
- Receipt of data to be processed must be validated for accuracy and checked that it has been properly collected. If a third party provides the data, assurances that the information is correct and properly collected may have to be sought.

3.2 Access to personal data

3.2.1 The Data Protection Act 1998 gives you the right to apply for a copy of data about yourself (Subject Access Request). You may, if you so wish, appoint someone (an agent) to apply on your behalf e.g. your parent or a solicitor.

When requesting a copy of your data you will be asked to provide a proof of identity (e.g. Service ID card, passport, photo card driving license etc). Full details of making a subject access request can be found in appendix E. The full process data can be found on appendix F.

4 Additional information

For guidance on the Employee Code of Conduct please refer to [SO/1/20](#).

For guidance on the Information Service General Responsibilities please refer to www.hantsfire.gov.uk/general-responsibilities.htm

For guidance on the Service Protective Marking please refer to [HFRS Protective Marking Scheme](#).

5 Appendices

[Appendix A](#) - The Eight Data Protection Principles (attached)

[Appendix B](#) – CCTV SO/11/5 (link to SO)

[Appendix C](#) – Images of people

[Appendix D](#) – A relevant filing system

[Appendix E](#) - Data subject request

[Appendix F](#) - Subject data access procedure FM 11/1/2 (link to FM)

SO/11/1 Appendix A - The eight Data Protection principles

Owner: Information Compliance Officer

Author: Service Information Compliance Officer

Date amended: 12/2012

Next review date: 12/2013

The Data Protection Act 1998 refers to "**Eight Data Protection Principles**". These rules governing the processing and use of personal information are:

1 Fairly and lawfully processed

1.1 The Service will, as far as is practicable, ensure that all individuals whose details it holds are aware of the way in which that information will be held, used and disclosed. Individuals will, where possible, be informed of the likely recipients of the information - whether the recipients are internal or external to the Service. Processing within the Service will be fair and lawful, and individuals will not be misled as to the uses to which the Service will put the information given.

1.2 Personal data shall not be processed unless at least one of certain conditions are met. The most relevant are:

- The Data Subject has given their consent to the processing.
- The processing is necessary either for the performance of a contract to which the Data Subject is a party or for the taking of steps or at the request of the Data Subject with a view to entering into a contract (this would cover payroll related activities).
- The processing is necessary for compliance with any legal obligation to which the data controller (the person responsible for the processing) is subject.
- The processing is necessary for the purposes of legitimate interest pursued by the data controller except where the Data Subject's fundamental rights prevail.

1.3 Sensitive personal data (see para 1.4) will only be processed where, in addition to one or more of the conditions of personal data above being met, at least one of certain other conditions is also met. Where an employer is relying on a "necessary" condition, they should ensure that the decision making process is well documented. The most relevant additional conditions are:

- The Data Subject has given their explicit consent to the processing of the personal data.
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment (this covers all employment related legislation such as discrimination, health and safety and immigration legislation).
- The processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings); is necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- The processing is necessary for medical purposes.
- The processing is necessary for ethnic monitoring purposes.

1.4 Sensitive personal data means personal data consisting of information as to:

- The racial or ethnic origin of the Data Subject.
- Their religious or other beliefs of a similar nature.
- Their political opinions.
- Trade Union membership.
- Their physical or mental health or condition.
- Their sexual orientation.

The commission or alleged commission by the Data Subject of any offence, or 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"

1.5 Data collection forms requiring personal information will contain a 'fair obtaining' statement giving details of the likely uses of the information and where information is collected in person or by telephone, the employee asking for the details will tell the individual how those details will be used. People are free to ask the person collecting the information why they want the details and what they will be used for.

Example of 'Fair Obtaining' statement:

Data Protection Legislation

The information you have provided will be held for the purposes of processing and administration and will be added to your personal file. Please notify us immediately of any changes so that we can keep your information up to date. Personal data may be disclosed to the Data Subject, data processors and, personnel staff. Occasionally we may be required by legislation to disclose data to Government Agencies such as the Anti-fraud Investigation Department.

1.6 The processing must be necessary for the purposes of legitimate interest pursued by the data controller except where the Data Subject's fundamental rights prevail. If a person's details are going to be used for 'auto-decision' processing (where a computer decides something based on a score or other information) the person will be told how the system works and whether the decision can be challenged.

1.7 If a person's details are to be processed for a purpose that does not appear on the Service's register entry (eg, some manual and/or non-contentious core processing) the individual will be given the information that would be necessary to make the processing fair and lawful.

2 Processed for limited purposes

2.1 The Service will not use or process personal information in any way that contravenes its notified purposes or in any way that would constitute a breach of Data Protection legislation.

2.2 When collecting personal data it should be explained to the Data Subject the purpose(s) for holding their details, the type of processing involved and whether it is likely to be passed to anyone. The Data Subject will then be free to choose whether or not to provide their personal details and will therefore provide their informed consent to process their personal data. However, certain personal data will be required by the HFRS if it is to operate as an efficient employer.

2.3 Where processing of personal data is carried out for the purposes of statistical or historical research and that data is not processed to support measures or decisions with respect to particular individuals, and in such a way that substantial damage or substantial distress is, or is likely to be caused to any Data Subject, such processing is not to be regarded as incompatible with the Second Principle.

2.4 The personal data processed may be kept indefinitely, notwithstanding the Fifth Principle, as long as the results of the research or any resulting statistics are not made available in a form, which identifies Data Subjects, and a Data Subject will not have those rights referred to as "Rights of Access".

3 Adequate, relevant and not excessive

3.1 The Service will not collect data from individuals where that information is excessive or irrelevant in relation to the notified purpose(s).

3.2 Details collected will be adequate for the specific purpose and no more. Excess information, such as date of birth and religion should not be requested unless it is essential to supply the service required, forms part of the information required for employment or is required by law.

3.3 Information collected, which becomes, over time or by virtue of changed purposes, irrelevant, or excessive, will be deleted.

4 Accurate

4.1 The Service will ensure, as far as is practicable, that the information held is accurate and up to date.

4.2 The intention is to check wherever possible the details given. Information received from third parties (i.e. other than the individual concerned or the Service) will carry a comment indicating the source.

4.3 Employees are required to notify changes to their personal details ([FM/1/2](#)).

4.4 Where a person informs the Service of a change of their own circumstances, such as home address or non-contentious data, their record(s) will be updated as soon as possible.

4.5 There should be regular audit trails to check the accuracy and quality of data being collected and entered into systems. Records should be regularly reviewed, amended when necessary, and passed through the retention process for that particular type of record.

4.6 Where the individual requests that information be changed and it is not possible to update it immediately, or where the new information needs to be checked for its accuracy or validity, a comment will be placed on the disputed record indicating the nature of the problem.

4.7 Every effort will be made to reach an amicable agreement on any disputed data. Where this is not possible the Service will implement the dispute procedure. Information on this is available from the Service Information Compliance Officer.

5 Not kept for longer than necessary

5.1 Information will only be held for as long as is necessary for the notified purpose(s) - after which the details will be deleted.

5.2 All staff processing personal data must conform to the HFRS Retention Policy ([Appendix E](#)) and destroy all unnecessary personal data in line with these procedures.

5.3 Retention periods should be regularly reviewed. Legal retention requirements for certain types of records have set standards to be obeyed. Any proposed changes to retention periods must be approved by the Information Compliance Officer.

5.4 In setting retention periods it is important to define a reasonable period of time for the class of records. It is not reasonable to retain records in case you might need them.

5.5 Where details of individuals are stored for long-term archive or historical reasons and where it is necessary to retain the personal detail within the records it will only be done within the

requirements of the legislation. In many cases personal details will be removed from the record so that individuals cannot be identified.

6 Processed within the individual's rights

6.1 Right of access

An employee has the right to be given:

- A description of all personal data held by the employer together with the purposes for which it is being processed.
- The recipients and the source of the personal data.
- A copy of personal data itself.
- To ask for incorrect data to be corrected.

6.2 Automated decisions

An employee has the right to be informed of the logic involved in decision taking where that decision is made solely by automated means, such as psychometric tests. The logic need not be disclosed if it constitutes a trade secret.

6.3 Third parties

There is no right of access where information would reveal the identity of a third party, unless:

- The consent of that third party is obtained,
- Or it is reasonable to proceed without consent,
- Or the third party is a health professional who has compiled or contributed to a health record.

6.4 Children have the right to subject access. However, a child will not always be able to make its own request. The way in which the subject access right will work in this situation depends on the general law relating to the legal capacity of children. There are few exceptions to this rule, such as data held for child protection or crime detection/ prevention purposes, but individuals will be able to have a copy of the permitted data held on them.

- A data user in England, Wales or Northern Ireland who receives a subject access request form by or on behalf of a child will need to judge whether the child understands the nature of the request.
- If the child does understand, he or she is entitled to exercise the right and the data user will reply to the child. A reply should be given to a request made on the child's behalf by a parent or guardian only if the data user is satisfied that the child has authorised the request.
- If the child does not understand, the parent or guardian is entitled to make the request on behalf of the child and to receive the reply. Parents or guardians should only make such a request in the interests of the child, not in their own interests.

6.5 All requests for access must be made in writing and HFRS reserves the right to charge the current fee of £10 regulated by the Data Protection Act 1998 for personal data access. (A special rule under the DPA for manual health records sets the maximum fee at £50). Once the request and fee has been received, HFRS must comply promptly and in any event within 40 days.

6.6 The Data Subject can ask HFRS not to use personal information about them for direct marketing or, anything likely to cause them unwarranted substantial damage or distress, or to

make decisions which significantly affect them, based solely on the automatic processing of data.

6.7 Automated decisions

In addition to the above rights of access, no decision, which significantly affects an employee, may be based solely on the processing of personal data by automatic means unless the employer either is undertaking such processing in response to a request of the employee or allows the employee to appeal against such a decision.

6.8 Exemptions to the right of access include:

6.8.1 Management forecasts and planning – where personal data is processed to assist the employer in the conduct of their business and subject access would be likely to prejudice the conduct of the business.

6.8.2 Negotiations – where subject access to information recording the intentions of the employer in negotiations with the employee would be likely to prejudice those negotiations.

6.8.3 Legal professional privilege – where data consists of information in respect of which such a claim could be maintained in legal proceedings.

6.8.4 The "Health Order" that restricts the rights of Data Subjects to gain access to information held about them which relates to physical or mental health, education records and social work records.

6.8.5 Confidential references - where personal data consist of a reference given or to be given in confidence by the data controller for the purposes of:

- the education, training or employment, or prospective education, training or employment, of the Data Subject,
- the appointment, or prospective appointment, of the Data Subject to any office, or
- the provision, or prospective provision, by the Data Subject of any service".

The Data Subject will **not be entitled** to request data from the reference provider. However, although there is no specific provision to deny the Data Subject's right of access to the same confidential reference where it is held on the recipient's file, if the exercise of access rights involved disclosure of the identity of the author of the reference, disclosure could not take place unless the author had given their consent. If the author has specifically stated that the reference was given in confidence, this would be a clear expression that consent has not been given to access by the Data Subject. In effect, this will block the Data Subject's right of access to the reference in the hands of the recipient.

6.9 Enforcement of rights

6.9.1 Complaint to the Information Commissioner – may lead to Enforcement or Information Notices.

6.9.2 Access - the court may order the employer to permit access by the employee to personal data.

6.9.3 Rectification, Blocking, Erasure and Destruction – the court may order the employer to take such action in relation to inaccurate data.

6.9.4 Compensation – the court may award compensation in respect of any breach of the legislation, which has resulted in loss or damage. Although under the legislation, damages for

distress will only be available where physical or economic damage has resulted, the European Commission has stated that damage should include psychological damage.

7 Secure

The Service has implemented appropriate security measures as required under the DPA.

7.1 Unauthorised staff and other individuals are prevented from gaining access to personal information.

7.2 Computer systems are installed with user-profile type password controls and where necessary, audit and access trails to establish that each user is fully authorised. In addition employees are fully informed about overall security procedures and the importance of their role within those procedures.

7.3 Electronic data is backed up.

7.4 Manual filing systems are to be held in secure locations and can only be accessed by authorised staff.

7.5 Security arrangements are reviewed regularly by Functional Data Managers, any breaches or potential weaknesses must be reported immediately to the Service Data Protection Officer who will arrange for an investigation to be conducted and where necessary further or alternative measures will be introduced to secure the data.

7.6 Redundant personal data will be destroyed using the Service's procedure for disposal of confidential waste. In general, paper waste is shredded and magnetic media (disks, tapes, etc) are either electronically wiped or physically destroyed beyond recovery.

7.7 Appropriate physical security is in place and all visitors have to report to reception areas to sign themselves in and out of the buildings. Visitors must be escorted at all times within Service buildings where information is used or stored.

8 Not transferred to countries without adequate protection


It is a specific requirement of the Data Protection Act 1998 that personal data is not transferred outside the European Economic Area (The EEA) without assured safeguards being met. The EEA consists of 15 European Union Member States together with Iceland, Liechtenstein and Norway. Accordingly personnel are instructed to ensure that no data is transferred outside the EEA. Where there exists a need to do so the Information Compliance Officer must be consulted before any such transfer takes place. The Information Compliance Officer must be informed of any unauthorised disclosure or breach of security, which will be dealt with under the Service's disciplinary procedures

SO/11/1 – Appendix B – SO/11/5 - CCTV

Author: Service Information Compliance Officer

Date reviewed: 12/2012

Next review date: 12/2013

This appendix can be found using the following link:  [SO/11/5](#)

SO/11/1 Appendix C - Images of people and commissioned photographer's contract

Owner: Information Compliance Officer
Author: Service Information Compliance Officer
Date amended: 12/2012
Next review date: 12/2013

1 Introduction

1.1 Since the introduction of the Data Protection Act 1998 care must be taken if photograph and video images are captured of clearly identifiable people and are to be processed, published or stored in a relevant filing system.

1.2 Images must be destroyed within two years of the date on the consent form, unless further consent is agreed. This is important if the publication will have a wide circulation or publicising an event.

2 Consent

2.1 Before you start taking images of people it must be made clear to the Data Subject:

- Why their image is being used.
- What the image will be used for.
- Who might look at the image.
- Where the image will be released and how.
- Obtain their consent.

2.2 You need consent (or parental consent for those under 18) when an individual is clearly recognisable in an image. You need to be particularly careful when dealing with children, so you **must** get permission from the parent, guardian or carer of any child or young person up to the age of 18. In exceptional circumstances a decision may need to be made on the individual case (e.g. the person may have left home but is under 18 years of age and therefore it may be difficult to get parental consent).

- If two parents disagree over consent for their child to appear in images then it has be treated if consent has **not** been given.
- If the parents agree to consent, but the child does not, then consent is regarded as **not** having been given.

2.3 If you are taking images at an event attended by large crowds, such as the "Fireshow", this is regarded as a public area so you do not need to get the permission of everyone in a crowd shot. People in the foreground are also considered to be in a public area, however, photographers must address those within earshot, stating where the photograph may be published and giving them the opportunity to move away.

2.4 If you want to use an image of a person which can only be captured at an instant, then you must get their verbal permission and record the fact that you have done so. You can record their consent on a Verbal Consent Form ([FM/11/1/6](#)) when you capture the image or when you return to your office.

2.5 Consent forms for:

- Consent to use image/video footage ([FM/11/1/6](#))

are available at www.hfrs.net or from the Information Compliance Officer..

3 Images

3.1 Existing images

The use of existing images for which consent was not obtained, ie, images obtained before the Act came into force, need careful justification before publication. Guidance to achieve a balanced decision includes:

- For what purpose was the original picture taken, eg, was it taken for a specific project?
- Where was the image taken, eg, in a public place?
- When was it taken, eg, was it taken of a child who could now be an adult?

3.2 Photograph libraries

Departmental photographic libraries must enable the checking of consent forms if re-using photographs. However, preparation must be made to destroy all photographs once consent has expired.

3.3 Agency images

If you get photographs from an agency, you must ask the agency to guarantee that permission has been granted. Wherever possible, however, you must use photographs that portray Hampshire people on Hampshire sites. You must also tell the agency how you will be using the photographs. Ultimately, however, it is your responsibility to ensure that the agency obtained permission from the people in the photographs, so you must get this in writing from the agency.

3.4 Staff images

Photographs taken for security reasons using a digital camera, to enable access to buildings, is a legitimate business purpose for processing personal data. However, unless the staff member agrees, these images cannot be used for any other purpose without consent. Departments may wish to display photographs of staff on HFRS.net (HFRS internal website) or notice boards (e.g. for staff recognition purposes.) The image is personal data and individuals may only give consent for their images to be accessed by their department. Their wish must be respected.

4 Commissioned photographer's contract

Ensure that all contracts drawn up with commissioned photographers include a data protection statement to include:

- Agreement to comply with the requirements set out within the Data Protection Act 1998.
- Agreement to take appropriate measures to prevent unauthorised or unlawful processing of personal data and against accidental loss, destruction of or damage to personal data (including photographs).
- Granting of consent has been recorded on their system or by the use of HFRS consent forms.

SO/11/1 Appendix D - Definition of a 'relevant filing system'

Owner: Information Compliance Officer
Author: Service Information Compliance Officer
Date amended: 12/2012
Next review date: 12/2013

Section 1(1) of the DPA defines a "**relevant filing system**" as "any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured either by reference to the individual or to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible".

The Information Commissioner issued (February 2004) the following clarification:

The statutory right to be given access to personal data will only apply if the filing system is structured in such a way as to allow the recipient of the request to either:

(a) know that there is a system in place which will allow the retrieval of file/s in the name of an individual (if such file/s exists); and know that the file/s will contain the category of personal data requested (if such data exists);

or

(b) know that there is a system in place which will allow the retrieval of file/s covering topics about individuals (eg, personnel type topics such as leave, sick notes, contracts etc.); and

know that the file/s are indexed /structured to allow the retrieval of information about a specific individual (if such information exists) (eg, the topic file is subdivided in alphabetical order of individual's names).

Where manual files fall within the definition of a "relevant filing system", the content will either be so sub-divided as to allow the searcher to go straight to the correct category and retrieve the information requested without a manual search, or will be so indexed as to allow a searcher to go directly to the relevant page/s.

A filing system containing files about individuals, or topics about individuals, where the content of each file is structured purely in chronological order **will not be a relevant filing system** as the files are not appropriately structured/ indexed/ divided or referenced to allow the retrieval of personal data without leafing through the file.

Personnel files and other manual files using individuals' names or unique identifiers as the file names, which are sub-divided/indexed to allow retrieval of personal data without a manual search (such as, sickness, absence, contact details etc.) are likely to be held in a "relevant filing system" for the purposes of the DPA. However, following the Durant judgment it is likely that **very few manual files will be covered by the provisions of the DPA.**

It is important to note that the Freedom of Information Act 2000 (FOI) will amend the DPA to expand the definition of "data" from January 1st 2005. As a result of the expanded definition, public sector bodies must ensure that the personal data they hold (including unstructured manual personal data **except** unstructured manual personnel records) must be accurate, up to date and accessible under DPA (Section 7). It should also be noted that the compensation and rectification provisions of the DPA will apply in respect of such data although so far as subject access fees are concerned, the charges under the FOI will apply.

Flowchart - is it a relevant filing system?

SO/11/1 Appendix E – Data subject request

Author: Service Information Compliance Officer

Date amended: 12/2012

Next review date: 12/2013

1 Procedure

1.1 The Data Subject, or their nominated representative must make requests in writing for access to personal data to the Service Information Compliance Officer. (Personal data will be sent to the Data Subject's address unless the contrary is indicated).

1.2 The Service will attempt to reply to subject access requests as quickly as possible and in all cases within the 40 days allowed by the Data Protection Act.

1.3 Repeat requests will be fulfilled unless the period between requests is deemed unreasonable, such as a second request received so soon after the first that it would be impossible for the details to have changed.

1.4 To expedite the procedure a guidance note:

1.5 The Information Compliance Officer will activate a secure manual file progress the request and liaise with the requestor.

1.6 The Information Compliance Officer will ensure:

Information provided is intelligible, and any reference codes are explained clearly;

- Ensure information identifying other individuals is deleted - unless their consent has been obtained in writing;
- Consider whether to explain if names/ identifying information about other individuals have been deleted due to consent being withheld or was unable to be obtained;
- Consider whether provision of information may cause serious harm to the individual or someone else if it is given. Professional advice may be sought on this.
- Consider if there are any reasons why information must be withheld e.g. prejudicial to crime and taxation investigations, national security; and
- When satisfied that information can be provided, photocopy the information and securely send it (eg recorded delivery) to the Data Subject with the Acknowledgement of Satisfaction ([FM/11/1/5](#))

1.7 If no information is held or has been withheld under exemptions, the Information Compliance Officer must send the letter to the Data Subject indicating that no information is held, or no information is held that the Service is required to give them. There is no requirement to explain why information has been withheld.

2 Complaint/grievance

2.1 If the Data Subject has indicated that the information about them is incorrect or inaccurate or are unhappy or have a grievance with HFRS about their request, the Information Compliance Officer should discuss it with them, and seek their consent to pass information on to the relevant department to deal with the root of the problem/ concerns.

2.2 Whenever possible, complaints will be written, dated and will include details of the complainant as well as a detailed account of the nature of the problem.

2.3 The Service will attempt to complete internal investigations within twenty days, and in every case the person will receive an acknowledgement as soon as possible after HFRS receives the complaint.

Information Compliance Officer
Hampshire Fire and Rescue Service Headquarters
Leigh Road
Eastleigh
SO50 9SJ

E-mail: <mailto:DP@hantsfire.gov.uk>

Telephone: 023 8062 6850 or 023 8064 4000 ext 3950

Appendix F - Subject data access procedure FM 11/1/2 (link to FM)

Author: Service Information Compliance Officer

Date amended: 12/2012

Next review date: 12/2013

This appendix can be found on the following link: [FM/11/1/2](#).