**Faculty of Public Health**

**Data Protection Guidance and Procedures Manual**

**November 2009 *(Reviewed February 2013)***

***Please note:***

***This document is currently under review to ensure it complies with the General Data Protection Regulation (GDPR) and***

***the current Data Protection Act***

***On completion of the review a revised policy document will be published to the FPH website.***

# Contents

A. Overview

B. Introduction to Data Protection

1. Data Protection Act 1998
2. Data Protection Definitions
3. The 8 Data Protection Principles

C. Data Protection - FPH procedures

1. Summary
2. FPH designated responsibilities
3. FPH employees responsibilities
4. FPH Data Subjects and Classes
5. Subject Consent
6. Data storage and maintenance
7. Data security
8. Subject Access Requests
9. Disclosure of Data
10. Data retention
11. Data disposal
12. Publication of information
13. FPH examinations

D. FPH Department Guidance – data retention

# A. Overview

This document provides an introduction to the Data Protection Act (the 'Act') and its principles, and outlines the FPH procedures and guidance developed in response to the Act.

The document supports the FPH Data Protection Policy approved by the FPH Board on 23rd September 2009. It has been primarily designed to serve as a guidance manual for FPH employees involved in the processing of personal data at FPH. However, it will be made available in electronic form to individuals whose personal data is held by FPH upon receipt of written request to the Chief Executive.

The procedures and guidance contained in sections C and D will be reviewed on an annual basis to ensure that they comply with the Act and other related laws, and to accommodate changes in FPH organisational policies and upgrades to FPH systems. They will form the basis of a staff training programme and staff induction programme in data protection.

The FPH Data Protection Policy is located on the FPH website and in the FPH Staff Handbook which is issued to all staff on joining FPH.

# B. Introduction to Data Protection

## 1. Data Protection Act 1998 – an overview

The Data Protection Act 1998 commenced on 1 March 2000, with most of its provisions being effective from 24 October 2001. It replaced and broadened the Data Protection Act 1984.

The purpose of the Act is to protect the rights and privacy of individuals, and to ensure that data about them are not processed without their knowledge and are processed with their consent wherever possible. The Act covers personal data relating to living individuals and defines a category of sensitive personal data which are subject to more stringent conditions on their processing than other personal data.

The Data Protection Act covers data held in electronic formats, and also applies to manual data which are held in what the Act calls a relevant filing system. [[1]](#footnote-1)

## 2. Data Protection Definitions

These are drawn from the guidance available on the Information Commissioner's website <http://www.informationcommissioner.gov.uk/>

### a. Personal data

Personal data means information about a living individual who can be identified from that information and other information which is in, or likely to come into, the data controller's possession. Personal data include information such as an individual's name, home and work addresses, educational background, images and photographs (including CCTV footage), expressions of opinion about the individual, and the intentions of the data controller in regard to the individual.

### b. Sensitive personal data

The Act defines categories of sensitive personal data, namely, personal data consisting of information as to:

(a) the racial or ethnic origin of the data subject; \*

(b) their political opinions;

(c) their religious beliefs or other beliefs of a similar nature;

(d) whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);

(e) their physical or mental health or condition; \*

(f) their sexual life;

(g) the commission or alleged commission by them of any offence; or

(h) 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.

\* indicates information routinely collected by FPH

### c. Data Subject

Data subject means "an individual who is the subject of personal data". A data subject must be a living individual. Organisations, such as companies and other corporate and unincorporated bodies of persons cannot, therefore, be data subjects. A data subject need not be a United Kingdom national or resident. Provided that the data controller is subject to the Act, rights with regard to personal data are available to every data subject, whatever their nationality or residence.

### d. Subject Access

Under the Data Protection Act, individuals can ask to see the information about themselves that is held on computer and in some paper records. If an individual wants to exercise this subject access right, they should write to the person or organisation that they believe is processing the data.

A subject access request must be made in writing and must be accompanied by the appropriate fee. In most cases, the maximum fee will be £10, but this can vary, particularly if the information requested is for health or educational records. If a subject access request is made to a credit reference agency, then the fee is £2, and the information must be provided within seven working days. A request must include enough information to enable the person or organisation to whom the subject is writing to satisfy itself as to their identity and to find the information. For education records and files (which may be held in hard copy) a fee of up to £50 is charged depending on the level of administrative work involved.

A reply must be received within 40 days as long as the necessary fee has been paid. A data controller should act promptly in requesting the fee or any further information necessary to fulfil the request. If a data controller is not processing personal information of which this individual is the data subject, the data controller must reply saying so[[2]](#footnote-2).

### e. Subject Consent

The process in which a Data Subject provides consent for their data to be processed by an individual or organisation.

### f. Data Controller

A person who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons. FPH as an organisation is the Data Controller and thus ultimately responsible for legal compliance.

### g. Processing

Processing, in relation to information or data, means obtaining, recording or holding the information or data (which includes, in relation to personal data, obtaining or recording the information to be contained in the data) or carrying out any operation or set of operations on the information or data, including -

* organisation, adaptation or alteration of the information or data;
* retrieval, consultation or use of the information or data (which, in relation to personal data, includes using the information contained in the data);
* disclosure of the information or data (which, in relation to personal data, includes disclosing the information contained in the data) by transmission, dissemination or otherwise making available, or alignment, combination, blocking, erasure or destruction of the information or data.

This definition incorporates, amongst other things, the concepts of "obtaining", "holding" and "disclosing". The definition in the Act is a compendious definition and it is difficult to envisage any action involving data which does not amount to processing within this definition.

### h. Disclosure of data

The process in which personal data is shared with a third party. Disclosure may be unlawful even if the third party is a family member of the data subject, or a local authority, government department or the police. The disclosure of personal data represents a form of processing of the data. This means that the conditions for fair and lawful processing of personal data and sensitive personal data set out in first Data Protection Principle must be met.

### i. Data security

Involves the precautions taken against the physical loss or damage of personal data, and the restriction of disclosure of personal data as outlined in the 7th Data Protection principle.

### j. Data retention

Relates to the period of time that personal data is retained. The Act 1998 does not specify periods for the retention of personal data. It is left to data controllers to decide how long personal data should be retained, taking into account the Data Protection Principles, business needs and any professional guidelines.

### k. Data disposal

The process by which personal data is destroyed. Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data.

## 3. The 8 Data Protection principles

The data protection act sets out 8 principles governing the use of personal information with which FPH must comply unless an exemption applies. The principles are in essence a code of good practice for processing personal data.

### a. The 8 principles

1. **Personal data shall be processed fairly and lawfully.**Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.
2. **Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.**Data obtained for specified purposes must not be used for a purpose that differs from those.
3. **Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.**Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.
4. **Personal data shall be accurate and, where necessary, kept up to date.**Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by FPH are accurate and up-to-date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate. Individuals should notify FPH of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of FPH to ensure that any notification regarding change of circumstances is noted and acted upon.
5. **Personal data shall be kept only for as long as necessary.**
6. **Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act**
7. **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.**
8. **Personal data shall not be transferred to a country or a territory outside the European Economic Area 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.**Data must not be transferred outside of the European Economic Area (EEA) – the 27 EU Member States together with Iceland , Liechtenstein and Norway – without the explicit consent of the individual. Members of FPH should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a website that can be accessed from outside the EEA.

### b. Individuals' rights

The Act gives rights to individuals in respect of personal data held about them by others.

The rights are:

* right to subject access;
* right to prevent processing likely to cause damage or distress;
* right to prevent processing for the purposes of direct marketing;
* rights in relation to automated decision taking;
* right to take action for compensation if the individual suffers damage by any contravention of the Act by the data controller;
* right to take action to rectify, block, erase or destroy inaccurate data.

### c. Right of subject access

Upon making a request in writing (which includes transmission by electronic means) and upon paying the appropriate fee to the data controller, an individual is entitled to be told by the data controller whether they or someone else on their behalf is processing that individual’s personal data, and if so, to be given a description of: -

* the personal data;
* the purposes for which they are being processed; and
* those to whom they are or may be disclosed.

The individual is also entitled to have communicated to them all the information which forms any such personal data. This information must be supplied in permanent form by way of a copy, except where the supply of a copy in permanent form is not possible or would involve disproportionate effort, or the data subject agrees otherwise.

"Disproportionate effort" is not defined in the Act. Accordingly, it will be a question of fact in each case as to whether the supply of information in permanent form amounts to disproportionate effort. Matters to be taken into account by the Information Commissioner may be the cost of provision of the information, the length of time it may take to provide the information, how difficult or otherwise it may be for the data controller to provide the information and also the size of the organisation of which the request has been made. Such matters will always be balanced against the effect on the data subject.

Further information on the Data Protection Act can be found at [http://www.dataprotection.gov.uk](http://www.dataprotection.gov.uk/)

# C. FPH Data Protection Guidelines

## 1. Summary

**STAFF ARE REMINDED TO TREAT PERSONAL DATA WITH CARE AND TO NEVER PASS ON PERSONAL INFORMATION TO UNAUTHORISED PERSONS**

1. Only use personal data for the purpose it was obtained;
2. Only hold personal data that is required for the purpose for which it was obtained;
3. Ensure the data you hold is accurate and up to date;
4. Destroy personal data once the purpose for which it was obtained has been concluded;
5. Keep sensitive personal data secure and safe;
6. Do not transfer personal data outside the EEA unless the transfer is already authorised;
7. Co-operate in a helpful and timely manner following the agreed FPH procedures as and when any data subject access request is received;
8. There is no such thing as a Data Protection emergency (except where someone's life or health may be at risk). You are well within your rights to stall a caller/enquirer whilst you seek further information and advice.

## 2. FPH designated responsibilities

**FPH as an organisation** is the Data Controller and thus ultimately responsible for legal compliance.

**The Chief Executive and the Trustees of FPH** are responsible for ensuring that Data Protection policy is adequate, correct and reviewed regularly.

**The Chief Executive, via the FPH’s Senior Management Team**, is responsible for ensuring that procedures and training are in place to ensure that the Data Protection Policy is put into practice.

**Heads of Department** together with department representatives on Data Protection Working Group are responsible for staff training, induction and implementation of procedures in individual Departments.

**The Head of Corporate Affairs** is the FPH Data Protection Officer and is responsible, under direction from the Chief Executive for reviewing policy, preparing procedures, assisting on request with guidance and training, ensuring that the statutory notification is up to date and for reviewing contracts with external suppliers to ensure that handling of our personal data is adequate and well documented. The Head of Corporate Affairs is supported by the staff and the Senior Management Team to undertake this work. All new staff will receive training in Data Protection.

**Individual staff** are responsible for care in following procedures, and for raising any queries, concerns or training needs which they might have.

## 3. FPH employee responsibilities

Staff are reminded that it is an offence to process personal data except in strict accordance with the eight principles of data protection and the rights of data subjects. Failure to comply with the Data Protection Act could result in the prosecution not only of FPH but also of the member of staff concerned. Data subjects may also sue for compensation for damage and any associated distress suffered as a result of loss or unauthorised destruction of data; unauthorised disclosure of, or access obtained to, data; or inaccurate data - i.e. data which is incorrect or misleading.

FPH cannot process personal data unless the data subject has given ***explicit*** consent to the processing. A data subject has to “opt in” to such processing and consent cannot be assumed even if it is a purpose for which FPH can process data or the data subject has willingly provided the information as part of an established process by FPH.

### Lawful processing

All staff who are concerned with, or have access to, personal data have an obligation to ensure that it is processed in accordance with the Act. This means, among other things, that staff must treat all data carefully and must not disclose personal data to unauthorised persons (e.g. the relatives of examination candidates). FPH does not authorise any member of staff or agent of FPH to hold or process any personal data on its behalf except as stated in the FPH Notification with the Information Commissioners Office. In cases of doubt or difficulty staff should in the first instance contact the FPH Data Protection Officer. Any request to disclose personal data where this is not already authorised or part of agreed procedures should be referred to a senior manager. This includes requests made by Officers, Boards or Committees, working groups or special interest groups.

Failure to comply with the policy is likely to result in action under the FPH Disciplinary Procedure.

Any member of staff requested to respond to a data subject access request should do so promptly and conscientiously. All possible data sources must be searched from main databases, to separate lists and to structured paper files. If in any doubt, speak to your line manager as how best to respond to the request. Failure to co-operate reasonably in order for FPH to respond to a subject access request would be regarded as a disciplinary matter.

## 4. FPH Data subjects and classes

In order to satisfy operational and legal obligations FPH processes and maintains personal data on a range of data subjects. These include:

* FPH members
* FPH staff including volunteers, agents, temporary and casual workers
* Previous and prospective employers of the staff and referees
* FPH suppliers
* Complainants, correspondents and enquirers
* Advisers, consultants and other professional experts
* Business of other contacts
* Employees of other organisations
* Relatives, guardians and associates of the data subject
* Donors and lenders

The classes of personal data obtained and processed by FPH include:

* **Personal details** – name, address, contact details, age, sex, date of birth
* **Education and training details** – academic records, qualifications, skills, training records, professional expertise, student record
* **Employment details** – employment and career history, recruitment and termination details, attendance records, health and safety records, performance appraisals, training records and security details
* **Financial details** – income, salary, insurance details and pension information
* **Goods or services provided**
* **Racial or ethnic origin**

## 5. Subject Consent

Wherever possible, personal data or sensitive personal data should be obtained, held, used or disclosed only where the individual has given consent. This means that the data subject has been fully informed of the intended processing and has signified their agreement without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. The individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, *explicit* written consent of the data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and sensitive data is obtained routinely by FPH (e.g. when a candidate signs a registration form; a new member returns an application for membership or when a new member of staff signs a contract of employment). Any FPH forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. FPH should abide by the stated purpose on any form in regard to how it stores, uses, discloses and maintains personal data.

It is particularly important to obtain specific consent if an individual's data are to be published on the Internet as such data can be accessed from all over the globe. Therefore, not gaining consent could contravene the eighth data protection principle i.e. transferred to a country or a territory outside the European Economic Area.

If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.

[Subject Access Request](Subject%20Access%20Request)

## 6. Data storage and maintenance

Information on data subjects should be stored on the central FPH Zara database. A central database avoids the need to hold separate lists of members and/or others which ensures that FPH can respond quickly to comply with a subject access request.

There may be instances where the records should be held separately such as a specific project work for FPH either working alone or with a collaborating partner/s. In these cases records should be destroyed after the activity or project is concluded. Each line manager should advise and authorise any records where it is not appropriate to hold the data on the FPH database.

Email records are held separately on an external system as it would be impractical for staff to pass all emails to a central source. Emails are automatically archived for a period of 3 years.

Each line manager should know what information is held and by whom. The Department must be confident that all the information about a single member can be readily accessed from a limited number of sources and does not rely on the presence of one or more individuals to respond to a subject access request.

Departments must ensure that personal data records are accurate and as up to date as possible.

## 7. Data security

All staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party.

All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

• in a lockable room with controlled access, or

• in a locked drawer or filing cabinet, or

• if computerised, password protected , or

• kept on disks which are themselves kept securely.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential within the relevant policies set out in the employee handbook. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

This policy also applies to staff and members who process personal data "off-site". Offsite processing presents a potentially greater risk of loss, theft or damage to personal data.

Further guidance on security is available in the documents on the shared drive in the IT Documents folderor in the IT Procedures public folder in Outlook.

## 8. Subject access requests

An individual is entitled to be informed by FPH if personal data is held about them. If this is the case, the individual is entitled to be supplied with a copy of any such information with necessary explanations: a description of that personal data, the purposes for which it is being or will be processed, and the recipients to whom the data is or may be disclosed. This is a “subject access request”.

FPH is not obliged to comply with a subject access request unless it is satisfied as to the identity of the person making the request and is able to locate the information which that person seeks. FPH has to comply with the request within 40 days, following receipt of appropriate payment and proof of identity, unless the supply of such information is not possible or would involve disproportionate effort. There are some other restrictions as well. Case law provides that people cannot simply ask to know “what personal information FPH holds about me” but must be specific about what is wanted, what processing or function it relates to, or the period concerned.

Individuals can make a subject access request by completing the [Subject Access Request Form](Subject%20Access%20Request) and submitting relevant payment and proof of identity. If FPH receives a subject access request, this will be directed to the FPH Data Controller in the first instance. Once the nature of the request is clear an acknowledgement will be made to the data subject informing them of the final date before which they can expect a response. The request will then be directed to the Department or individual who it is thought to hold the relevant data and can respond to the request. The response is to be made to the FPH Data Controller who will reply to the person making the request.

## 9. Disclosure of Data

### a. General

* Staff should exercise caution when asked to disclose personal data held on another individual to a third party and follow FPH procedures outlined in this manual;
* Staff must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police.

### b. Legitimate disclosure of personal data

Personal data may be legitimately disclosed where one of the following conditions apply:

* the individual has given their consent (e.g. a candidate/member of staff/FPH member has consented to FPH corresponding with a named third party);
* where the disclosure is in the legitimate interests of FPH (e.g. disclosure to staff - personal information can be disclosed to other FPH staff if it is clear that those members of staff require the information to enable them to perform their jobs);
* where FPH is legally obliged to disclose the data (e.g. ethnic minority and disability monitoring);
* where disclosure of data is required for the performance of a contract (e.g. informing a sponsor of changes/withdrawal etc).

### c. Disclosure of personal data without consent

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

* to safeguard national security;
* prevention or detection of crime including the apprehension or prosecution of offenders;
* assessment or collection of tax duty;
* discharge of regulatory functions (includes health, safety and welfare of persons at work);
* to prevent serious harm to a third party;
* to protect the vital interests of the individual - this refers to life and death situations.

Requests must be supported by appropriate paperwork. It should be noted that FPH carries out very few functions which are required by statute.

### d. Disclosing sensitive personal data

In accordance with Principle 1 of the Data Protection Act, sensitive personal data should only be disclosed if one of the conditions set out above for disclosure of data and one of the conditions set out in Schedule 3 to the Act are met. The most likely conditions (of Schedule 3) applicable to the disclosure (over the telephone) of sensitive candidate or staff data to third parties are:

* the candidate, member of staff or FPH member has given their explicit (ideally written) consent.
* disclosure is in the vital interests of the candidate, member of staff or FPH member (e.g. information relating to a medical condition may be disclosed in a life or death situation).

### e. Disclosing personal data overseas

In accordance with Principle 8 of the Data Protection Act, personal data should only be disclosed outside of the EEA (the EU Member States together with Iceland, Liechtenstein and Norway) if one of the conditions set out in Schedule 4 are met. The most likely conditions applicable to the disclosure (over the telephone) of candidate, staff or FPH member data to third parties overseas are:

* the candidate, member of staff or FPH member has given their explicit (ideally written) consent;
* disclosure is required for performance of a contract;
* disclosure is necessary for the purpose of any legal proceedings.

### f. Disclosure of staff data

A colleague's work contact details can be disclosed in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of FPH business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the person concerned.

### g. Data disclosure and partnership working

FPH is an independent organisation and therefore not part of the NHS or any government department or agency even though we do work with such departments or agencies from time to time and projects can be funded by such bodies. Where we do work with others there should always be very clear statements about ownership, disclosure, storage and destruction of personal data in the documents governing the arrangement such as contracts or agreements. You should not enter into any contractual arrangements with any individual or person without consulting your line manager. Please remember that it is not necessary to sign a document to enter into a contractual arrangement.

### h. Data disclosure to the police

Disclosures to the Police are NOT compulsory except in cases where FPH is served with a Court Order requiring information. However, Section 29 of the Data Protection Act 1998 does allow FPH to release information to the Police WITHOUT the consent of the data subject in LIMITED circumstances. Such disclosures should only be made if the Police confirm that they wish to contact a named individual about a specific criminal investigation and where FPH believes that failure to release the information would prejudice the investigation. If you are contacted by the Police and are not sure how to deal with their request you can get in touch with a senior manager or the Data Protection Officer for advice on how to deal with the enquiry.

The Police MUST request the information from FPH in writing. You are NOT obliged to release information to the Police over the telephone. Most Police Forces will have their own request form, which should always include:

1. a statement confirming that the information requested is required for the purposes covered in Section 29;
2. a brief outline of the nature of the investigation;
3. the data subject's role in that investigation;
4. the signature of the investigating officer.

### i. FPH data disclosure procedures

* **An enquiry is received as to whether a named individual is a member of FPH:**
  + Ask the enquirer why the information is required.
  + If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of FPH may constitute an unauthorised disclosure.
  + If the member’s details are published on FPH website then certain details may have already been disclosed. In this situation, refer the enquirer to the website.
  + Please note that even confirming whether or not a person is a member of FPH or a member of FPH staff could be a potential breach of the Act.
* **A request for information is received via telephone**
  + Unless consent has been obtained from the data subject, information should not be disclosed over the telephone.
  + The enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.
  + Ask the enquirer to submit their request in writing (where appropriate on headed paper) providing you with time to check whether or not the request is legitimate and, where possible, obtain consent for the disclosure from the member of staff or candidate about whom information is requested. You should, wherever possible, reply to the request in writing.
  + As an alternative to disclosing personal data, FPH may offer to do one of the following:
    - pass a message to the data subject asking them to contact the enquirer;
    - accept a sealed envelope/incoming email message and attempt to forward it to the data subject.
  + Please remember to inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of FPH".
* **Urgent request received for discloser of information via telephone**
  + FPH recognises that in some, exceptional situations, time constraints and other factors make it a necessity to disclose information over the telephone.
  + Good practice is considered to be only releasing information to those individuals who have access to a unique identifier (staff or member number) or know at least three identifying data (e.g. name, address and date of birth) about the data subject. This should minimise the potential for damages because a relationship between the data subject and the caller has been established.
  + If you find yourself in a position where it is necessary to disclose information over the telephone, you should take a contact number and ring the enquirer back. This will go some way to ensuring that the caller is who he or she claims to be.
  + Even the above procedures could be subject to fraud and should only be used when no other alternative exists. In such cases, FPH should at least be regarded as having taken reasonable precaution given the circumstances - i.e. that the security in place was appropriate to the risk involved in unlawful processing of data. As always, particular care should be taken when disclosing sensitive personal data or information that could potentially cause the candidate, member of staff or FPH member to suffer subsequent damage and/or distress.
* **Request received for an FPH mailing list**
  + This will generally not be agreed (except lists of DsPH and HoADs).
  + Arrangements have been made with the provider of FPH's mailings to release limited data for the purpose of each monthly mailing.
  + Under the terms of some project and other arrangements, release of certain FPH data may be agreed but this must be covered by a contract, agreement or other arrangements that control and limit the disclosure and use of that data.
* **When you receive a call from someone claiming to be a candidate/FPH member**
  + You may receive telephone calls from individuals claiming to be candidates/FPH members and asking for some personal data. Unless you are 100% sure that the person on the line is who they claim to be, you should not disclose information over the telephone.
  + You are advised to ask for identifying details e.g. the candidate's/FPH member's id number, home address and date of birth before proceeding with the call. If the caller can provide the details accurately, make a note of the information that they require and inform them that you will send it to their email address. If this is not possible, you should send the information to them at an address recorded on the FPH database. If the caller insists that they need the information urgently, you may take a contact telephone number and call them back with the information.
* **When you receive a request for examination results over the telephone**
  + Examination results are never given out over the telephone and email is only used in exceptional circumstances.
* **When you receive a request for a reference over the telephone**
  + Giving references over the telephone is not usually recommended. However, this is acceptable if you have been specifically asked by a candidate, member of staff or FPH member to provide a reference at short notice.
  + The identity of the person requesting the reference should always be confirmed prior to disclosure. As a minimum security measure it is recommended that you ring the enquirer back to check that they are who they claim to be.
  + When disclosing information in the form of a personal reference please ensure that:
    - the information you disclose is FACTUALLY correct;
    - the disclosure is kept to a minimum;
    - sensitive data (e.g. details of health to explain absences from FPH) are **not** disclosed without the explicit consent of the candidate, member of staff or FPH member;
    - where opinions about a person's suitability are disclosed, your comments are defensible and justifiable on reasonable grounds;
    - if you are unable or unwilling to give a reference, such a refusal is communicated carefully, without, in effect, implying a negative reference.
* **How to manage difficult callers/requests**
  + The purpose of the Act is to protect the rights and privacy of individuals with regard to their personal information.
  + At times you may feel like you are being obstructive to callers asking for information about examination candidates or FPH members. In these cases, explain that you are following the requirements of the Data Protection Act. If you follow these guidelines in a courteous and professional manner, in most circumstances you should not experience any problems.
  + If you are faced with a particularly difficult caller, do your best to diffuse the situation without losing your temper. Explain that you are following FPH guidance and that by providing the information (at all or over the telephone for example), you could be breaking the law.

## 10. Data retention

FPH discourages the retention of personal data for longer than it is required. Considerable amounts of data are collected on FPH Fellows and members, examination candidates and staff. However, once a member of staff, FPH member or candidate has left, it will not be necessary to retain all the information held on them. Some data will need to be kept for longer periods than others. FPH has established policy and procedures for [retention and disposal of records](#Retention). If you are in any doubt, please consult your line manager.

In general, electronic records containing information about individual members/candidates are kept indefinitely on FPH database. Information would typically include name and address, exams taken and examination results. Departments should regularly review the personal files on individuals including members and candidates

Further information on FPH data retention procedures are outlined in section D of this manual.

## 11. Data disposal

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion). As far as the last of these is concerned, please ensure that the data (held in documents, files, folders or emails) is deleted from **all** electronic storage areas including recycle bins, "deleted" stores, "sent boxes" etc.

As mentioned elsewhere in this guidance, a subject access request will require FPH to search all possible sources of personal data about the data subject within the criteria (e.g. date, subject matter) that is specified by the data subject.

Further information on data disposal procedures is contained in section D of this manual.

## 12. Publication of information by FPH

FPH publishes a number of items that can include personal data of both FPH members and its staff. These currently include (and may be extended):

* FPH quarterly newsletter ph.com (such as authors of features);
* FPH annual report;
* Internal telephone directory;
* Candidate pass lists;
* Members and staff information on FPH website (including photographs) such as officers, advisors, departmental staff;
* Quarterly member mailings;
* e-bulletins;
* Press and PR information (including feature pieces, press releases etc);
* Policy briefing statements;
* Any other published information issued by FPH (such as ad hoc reports and statements).

It is recognised that there might be occasions when a member of staff, a candidate, a FPH Member, or a lay member of FPH, requests that their personal details remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of having their details including within any published information (printed, online or otherwise).In such instances, FPH should comply with the request and ensure that appropriate action is taken.

### a. Guidance on the use of photographs/video in publicity/promotional material

General photographs

If individuals are not readily identifiable from the photograph and it seems unlikely that any damage or distress will result from such inclusion then it will not be necessary to obtain consent. Therefore, FPH will not need to seek consent from members and *staff* whose images appear as incidental detail in publicity photographs for the use of their image.

Photographs of large group activities

Where photographs are to be taken of a large group activity, e.g. at the FPH annual conference, notices informing the audience that the session/event is being filmed/photographed should be displayed within the space (walls and doors of the room) so that individuals may leave the room briefly if they do not wish to appear in the photographs/ video footage. Contact details of a FPH member of staff will be provided on the notice in case of any queries or concerns.

Photographs of small groups/individuals

Where photographs are to be taken of a single individual, or a small group of individuals, where individuals are the main subject of the photograph (even if they are not identified by name), consent should be sought before any photographs are taken. When gaining consent, it is important to ensure that individuals are informed of the purpose for which the images will be used for (e.g. whether and where they will be printed and who will have access to them). In most cases, verbal consent is all that will be required although photographers may wish to use a standard release form, to be signed by the subject(s), to ensure that they have appropriate consent.

Publishing photographs on the web

Publishing on the internet potentially transfers personal data outside of the EEA for which rules on gaining consent from individuals are much stricter.

However, FPH members are located all around the world and the internet is the most efficient, inclusive and widely available communication channel to keep them up-to-date on various FPH activities. For instance, publishing photographs of the FPH Annual Conference speakers and delegates on the web is a necessary way to ensure that the members and other interested parties who cannot attend still feel part of the event.

If photographs of specified subjects (except where *staff/member* images appear as incidental detail) i.e. not of large groups are to be published on the internet, verbal consent should be obtained. If the subject is concerned, a standard release form can be used.

Publishing video material on the web

FPH will at times make video material available on its website, for instance to showcase the highlights of its Annual Conference for the benefit of people who cannot attend and other interested parties such as charities and the media. FPH will inform the speakers prior to filming that the event is to be filmed and made available on the internet, and seek their prior consent accordingly.

## 13. FPH Examinations

### a. Exam scripts

Exam scripts are exempt from Subject Access Request provisions. This means that FPH is NOT obliged to provide candidates with original or copies of exam scripts upon request.

### b. Examiners' comments

Whilst exam scripts are specifically exempt from Subject Access Requests, comments made by examiners are not. Candidates are entitled to a copy of all comments recorded by both internal and external examiners. If comments are made directly onto the examination script, and FPH chooses NOT to make the full script available upon request, the comments must be reproduced onto a separate form. It is therefore recommended to examiners that any comments should be made on attached sheets, rather than directly onto examination scripts.

In all cases, examiners' comments must be provided to candidates in "intelligible form" this may mean providing a "word processed" version if hand-written comments are potentially illegible.

All examiners are reminded that comments are subject to disclosure under data protection legislation and will be provided to candidates if requested. Examiners should therefore ensure that all comments can be justified and that no careless remarks are made on exam scripts, in emails/memos to colleagues, or on mark sheets. Any informal notes passed between examiners in the course of marking an examination script should be disposed of securely once the results and appeals processes have concluded and there is genuinely no need for the notes to be retained.

### c. Examination meeting correspondence

Candidates have the right to request copies of the relevant sections (i.e. relating to them) of minutes of meetings at which their results are discussed (this includes recorded discussion of impaired performance claims). FPH must provide a copy of the report (or relevant sections) within 40 days after the official release of results.

Copies of meeting minutes have to be disclosed even if candidates are not actually discussed by name. This is because the data can be linked back to the candidate using other information held by FPH (typically the candidate id number).

If meeting minutes contain information relating to third parties (typically other candidates), this data should be anonymised or removed before releasing the report to the candidate that has made the request. In some cases, it may be necessary to obtain consent from a third party. If a third party cannot be contacted or refuses to give consent, FPH may still disclose the report if it deems this to be reasonable (this will depend on duty of confidentiality owed to the third party).

It should be noted that, where the third party is a member of FPH staff, lay member, actor or an external examiner who has given their opinion of a candidate in a professional capacity, the Information Commissioner is likely to consider refusal of consent as unreasonable. Therefore members of staff and external examiners are advised that opinions expressed in a professional capacity may well be disclosed if requested, and confidentiality cannot be guaranteed. External Examiners will be informed of this possibility on appointment, or at the point at which they are asked to supply their report(s)/comments.

### d. Automated marking

FPH do not maintain any system of assessment based entirely on automated means. If candidates request a manual review of any marks generated by automatic means (such as optical mark reading), a fee may be charged.

**e. Publication and release of results**

Under the Data Protection Act, FPH has an obligation to explain to candidates where their results may be published. The Information Commissioners Office (ICO) has agreed that educational institutions have a legitimate interest to publish examination results for educational/training purposes, and FPH will inform all Training Programme Directors and Faculty Advisors of MFPH examination results.

FPH will also publish a list of all the successful candidates on the FPH website. However, explicit consent should be sought from candidates where it is intended to publish results on the Internet, and a mechanism is therefore provided for candidates to exercise their right for their results not to be displayed. This will be effected by including an "opt out" section on application forms. These preferences will be recorded on the database and FPH will abide by those preferences in the publication of examination results. The reason for this is that the publication of results on the Internet represents a transfer outside of the EEA and could potentially be in breach of Principle 8 of the Data Protection Act.

If a candidate asks to see a copy of their results, FPH must provide access to all examination/assessment marks within 40 days after the official release of results. This extends to all candidates, regardless of whether or not they owe FPH any money. Candidates can request a hard copy of the information held, in which case a written statement or printout of results will have to be provided.

As there is no sure way of confirming the identity of a caller, the risk of unauthorised disclosure of examination results over the telephone is high. Therefore **examination results should never be released over the telephone.**

### f. Candidates with disabilities

Special care should be taken to ensure that information relating to candidates with disabilities or those who require reasonable adjustments is not disclosed without the candidates' informed consent. Therefore, it is necessary to tell the candidate concerned why there is a need to disclose information, who will have access to the information, and the likely consequences of giving or withholding consent. Information relating to additional needs should be obtained and shared only on a "need to know" basis (e.g. Assistant Academic Registrar, Training Programme Directors, relevant examiners and invigilators).

If consent is not given, this should be respected and information should not be disclosed. You should inform candidates of the consequences of not giving their consent as this could seriously *affect* your ability to arrange appropriate examination procedures which they might be entitled to (such as extra time allowances).

# D. Department guidance on data retention

## 1. Department checklist for managing data

### a. What paper/electronic records must be kept

To identify which records FPH must or need to keep, it is important to consider the following:

1. **What do FPH need documented? What records/documents are part of FPH work processes? What records are you required to keep?** This will include equal opportunities, application forms, Form of Faith, address changes (i.e. yellow form), curriculum vitae etc.
2. **Look at each type of record and decide why it is created and maintained.** FPH is required to create and maintain records for a number of valid reasons, including organisation policy and procedures. This will include membership files, Education and Training files, staff files, project files, minutes, accounts and so on.
3. **You may find that many of the records on the list for FPH are active files maintained for convenience or reference material.** Reference and personal convenience are valid reasons for keeping records. Frequently, the only justifications for maintaining files are personal ones, such as “I need the records for reference”, “Somebody may ask for it”.
4. **To determine which records must be kept, focus on the files that directly support your department’s mission, FPH history (e.g. Faculty name changes, Royal College status) or administration.** These are records, without which FPH and its staff could not function, and these are the ones that need to be controlled.

### b. Filing guidelines for departmental paper records

* A single copy of an item should be kept on file. **ALL** previous copies to be removed from the file and securely destroyed as that information would then be considered inaccurate.
* Items within a file should be in chronological order with the most recent at the front.
* Ensure that all duplicates and drafts are removed and securely destroyed when working with a file.
* When archiving a file all duplicates, drafts, printed matter (i.e. emails), curriculum vitae and general correspondence should be taken out.
* Do not keep files called **‘General’** or **‘Miscellaneous’.**
* Hand written items should be legible.
* Paper clips should be removed and replaced by staples.
* Ensure you have a record of all files’ whereabouts when taken out of the filing system.

### c. What not to keep (paper/electronic records)

* Manuscripts, typescripts and drafts of reports and other papers unless they indicate substantial changes in drafting;
* Duplicate or multiple copies of anything – unless necessary e.g. in case of Public Health Today or any other publications;
* Any correspondence that has no value once it is no longer current, such as letters of acknowledgement, meeting and travel arrangements, invitations, acceptances, apologies and similar material;
* Papers relating to other organisations unless they have a direct bearing on the work of FPH;
* Brochures, trade information, mail shots and other items sent for information – unless deemed necessary by the department;
* Anything ‘just in case';
* If in doubt ask your line manager or the Data Protection Officer.

### d. What to keep while in active use (paper/electronic records)

* Complete sets of minutes of current committees and other key bodies;
* Anything that might be required as legal evidence, e.g. contracts, title deeds and deeds relating to conferences and grants;
* Correspondence and other supporting material for new initiatives and major decisions, e.g. a new committee, prize, lecture or working group, including anything that expresses a dissenting viewpoint;
* Current reports, policy statements and guidelines;
* Programmes for FPH meetings and conferences;
* Financial, personnel and property management records in accordance with current legislations;
* Letters that represent considerable research that set out key work and decisions and that support key legal and administrative papers.

### e. What to transfer to the FPH offsite storage facility

**Offsite storage services are currently provided by Iron Mountain**(Mr Quinton Gush T: 08445 601023).

* Anything prior to 2003 (when the Faculty was called The Faculty of Community Medicine (FCM) or The Faculty of Public Health Medicine (FPHM));
* Documentation on working parties and similar bodies that no longer exist;
* Documentation representing source material for FPH initiatives or projects;
* Superseded or withdrawn guidelines, leaflets, pamphlets and similar material produced by FPH.

## 2. Roles and Responsibilities

### SMT members:

1. Take responsibility for the implementation of the Data Retention Policy within their department/ remit;
2. Ensure that appropriate systems are in place, and that adequate resources are available within their individual departments for meeting records management requirements;
3. Take responsibility for ensuring that all other FPH policies, practices, systems, and procedures are consistent with the policy;
4. Ensure that Document Data Retention Policy responsibilities are included in procedure manuals and job descriptions for all staff.

### Members of staff:

1. Take responsibility for the records dealt with on a daily basis;
2. Familiarise themselves with, and adhere to, the FPH data retention policy. If unsure, ask their line manager;
3. Ensure not to duplicate work. Staff should go through and weed all electronic files and accumulated paperwork in accordance to the data retention policy and do the relevant audits as per a schedule set up by line managers and the Data Protection Officer.
4. After handing in notice of termination of contract (staff or suppliers), ensure all paper and electronic files are weeded and any records for archiving are dealt with accordingly. Ensure line managers are aware of any documents or records not dealt with during any hand over.

## 3. List of Department documents and retention period

### Chief Executive

|  |  |  |
| --- | --- | --- |
| CHIEF EXECUTIVE***:- Employee Records*** | | |
| ***DOCUMENTS*** | ***RETENTION PERIOD*** | ***REASON FOR RETENTION PERIOD & COMMENTS*** |
| Staff personnel records of employment | **7** years after employment ceases | Statute of Limitations |
| Applications for jobs-where the candidate is unsuccessful | **1** month after notifying the unsuccessful candidate | Guidelines suggest three months after notifying the unsuccessful candidate. The Equalities Act 2010. There is a one year limitation for defamation actions under the Limitations Act. |
| Sickness records | **3** years after the end of each tax year for Statutory Sick Pay purposes |  |
| Accident records | **3** years from the date of incident | Personal injury actions must generally be commenced within 3 years of the injury but Health & Safety records may need to be kept longer. |
| Health & Safety records | **6** years after employment ceased | The Occupational nurse has records of all staff regarding Health & Safety and should be informed of staff leaving to ensure she archives the records accordingly. |

### Business Management

|  |  |  |
| --- | --- | --- |
| Corporate Affairs***:- Committee minutes and Papers*** | | |
| ***DOCUMENTS*** | ***RETENTION PERIOD*** | ***REASON FOR RETENTION PERIOD & COMMENTS*** |
| All minutes and agendas | Final minutes and agendas to be transferred onto the central sever | Any hard copy versions of papers or previous drafts to be securely destroyed or deleted |
| Committee papers | Final committee papers to be transferred onto the central server | It is necessary to retain committee minutes and papers in perpetuity both as an historical record and as the minimum record of decisions made. Any hard copy versions of papers or previous drafts to be securely destroyed or deleted |
| Contracts with customers, suppliers or agents | **6** years after expiry or termination of the contract | 6 years is the Statute of Limitations within which proceedings founded on a contract may be brought. Currently all contracts and SLA are kept by the person dealing with the company or running the project. Shortly an Access database will be developed and all contracts and SLA will be stored and updated regularly. |

|  |  |  |
| --- | --- | --- |
| Corporate Affairs***:- Salaries, Subscriptions, Accounts*** | | |
| ***DOCUMENTS*** | ***RETENTION PERIOD*** | ***REASON FOR RETENTION PERIOD & REASON FOR RETENTION PERIOD & COMMENTS*** |
| Legal Requirements |  | By Statute of Limitations and the Charities Act, documentation regarding *Capital items (Legal and Government)* has to be retained for a minimum of 10 years with *Non-Capital items* being retained for a minimum of 7 years. The policy for FPH should therefore be to retain all documentation for a minimum of 10 years unless otherwise stated. Apply strict checks to determine the length of time information is held in line with our Document Retention and Disposal Policy. |
| Capital expenditure  Restricted Fund | Indefinitely  Indefinitely. | Commercial considerations  To be archived in the vault for 6 years and then transferred to offsite storage. |
| Direct Debit Mandate details  Subscription records  Salary Link | To be kept whilst member is paying subscription by direct debit  **5** years after ceasing membership  Put relevant notes onto the interaction screen and immediately destroy proof of income securely. | Security information of all paper copies not sent to the relevant bank deleted immediately but copies of all necessary information retained. All electronic details should be securely filed away and archived if not paying subscriptions by direct debit and shall not be kept for any longer than is necessary for the purpose.  Salary link requires proof of income and once seen and noted, and the relevant notes filed by finance, it’s securely destroyed and no copies are to be kept for any reason. |
| Supporting documentation for tax returns: VAT  Corporation Tax  PAYE  Payroll | **7** years from the end of the tax year  **7** years from the end of the tax year for which the company may be required to deliver a tax return  **7** years from the end of the tax year  Retain original documentation for 7 years after expiry or termination of the contract then securely destroyed. | Note in general that where there is an enquiry into a tax return, records should be retained until the enquiry is complete. These documents will be archived accordingly.  Taxes Management Act. However it does get retained by the Inland Revenue online indefinitely.  Statute of Limitations and Taxes Management Act. Archived on the Faculty Premises in the secured archive. |
| Annual FPH accounts | All accounts are to be retained on the premises in the Vault for 7 years from the end of the tax year and then securely destroyed accordingly. | Under the Companies Act 1985 & 1989 accounting records must be retained for a minimum of 7 years from the date they are made. |
| All supplier invoices, expense claims with supporting documents and bank statements  Instructions to bank i.e. Officers signatures, Change of Treasurer etc. | Scanned onto computer on an annual basis retaining original documentation for 7 years then securely destroyed.  Indefinitely | Once scanned they will be archived on the Faculty Premises in the Vault.  Copies should be scanned and stored on Disk/Optical scanning, in order to have a record of all Officers through the Faculty existence. An Officer can be in office for a minimum of 3 years. |
| Investments certificates, ledger and Fixed assets register | Indefinitely |  |
| Management Accounts | Archive each year onto Computer retaining originals for only one year. | This includes pre budget and actual spent. Budgets are done on SAGE and therefore are stored electronically. Keep electronic copies for no less than 36 months and Sage Ledger for 10 years. |

|  |  |  |
| --- | --- | --- |
| INFORMATION TECHNOLOGY**:** | | |
| ***DOCUMENTS*** | ***RETENTION PERIOD*** | ***REASON FOR RETENTION PERIOD & COMMENTS*** |
| Risk Register | To be maintained electronically |  |
| Message Labs  Email correspondence not backed up by Postini | Default setting is 3 years from date created | Message Labs was replaced in May this year once we moved to the hosted IT system. The existing Message Labs data has been archived to Outlook Data Files – with emails grouped by date. These will be retained by our IT Suppliers and can be accessed on request.  MS Exchange 2010 has its own archiving facility but we also use Postini. |
| Software Licences | Keep a electronic register indefinitely | Most licencing is now provided via out hosted services – on a Subscriber Access License (SAL) basis so we only rent the applications for as long as necessary. Licence agreements are then held byt our IT provider. Legacy licence information is held electronically. |
| Back ups | Keep for 7 years from date of creation. | Backups are preformed nightly and transferred electronically to an offsite location. Most IT support companies do a 3month cycle of backup – we have requested that our current nightly backups are kept for the first year, then on the 12month anniversary reduce to one backup for each month and keep until such time as we decide destroy them which will be after a 7yr term. The finance system has yearend backups which are backed up nightly. |

### Health Policy and Advocacy

|  |  |  |
| --- | --- | --- |
| Health Policy and Advocacy***:-*** | | |
| ***DOCUMENTS*** | ***RETENTION PERIOD*** | ***REASON FOR RETENTION PERIOD & COMMENTS*** |
| All minutes and action notes | Final minutes and agendas to be transferred onto the central sever | Any hard copy versions of papers or previous drafts to be securely destroyed or deleted |
| Committee papers | Final committee papers to be transferred onto the central server | It is necessary to retain committee minutes and papers in perpetuity both as an historical record and as the minimum record of decisions made. Any hard copy versions of papers or previous drafts to be securely destroyed or deleted |
| Electronic Bulletin  Public Health Today, Journals and Publications  Website  Letters and invites to stakeholders  Press statements and releases  Conference material – e.g. handbook | Transfer onto central server  Keep 5 hard copies for reference of all ph.com, Journals and Publications indefinitely.  6 years after expiry or termination of the contract  Maintain final copies on the central server  Maintain final copies on the central server  Three years for one or two hard copies of the handbook; keep discs of photos and conference presentations indefinitely; important correspondence is kept electronically on the Y drive and can be transferred to a disc if needed. | All correspondence with authors, corrections and proofs relating to each issue should be kept.  The Service Level Agreement (SLA) between FPH and the website provider should be kept as a hard copy for the records then scanned and securely destroyed.  This refers to any important correspondence by the PA&C e.g. within partnership and advocacy work. |

### Education and Training

**Specialty Registrars, examination candidates not in training and examiner files.**

Information held on these files **may** include:

* Personal and contact details: name, date of birth, home, correspondence and term-time address, telephone numbers (including mobile number), e-mail address, gender, age, ethnicity, disability;
* Academic/Training Record: what training programme trainees are on, what placements they have been on, what qualifications they have. The start and end dates of each period of study, periods of intercalation, examination results and training number;
* Copies of correspondence sent and received;
* Copies of forms relating to withdrawal, intercalation, transfer;
* Copies of claims for mitigating circumstances (together with supporting documentation), letters and forms in relation to cause for concern, disciplinaries, appeals and complaints.

Note: Equal Opportunities Forms & Curriculum Vitaes - As these could be classified as sensitive data only the most recent/current copy should be kept. All previous copies should be returned to the subject concerned or securely destroyed.

|  |  |  |
| --- | --- | --- |
| EDUCATION & TRAINING***:- Training, Examinations,*** | | |
| ***DOCUMENTS*** | ***RETENTION PERIOD*** | ***REASON FOR RETENTION PERIOD & COMMENTS*** |
| Specialty Registrar files  Files for examination candidates not in training  Specialty Registrar file  Trainees leaving a training post before completion and examination files for candidates not in training.  Files for examination candidates not in training | Personal/contact details and approved training posts are to be maintained on the database indefinitely.  Specialty Registrar file is to be archived onsite for 1 year after receiving CCT. Then scanned and maintained on the central X drive. Hard copies will be securely destroyed.  A summary of the file may be kept indefinitely.  Files should be archived onsite for one year and scanned and maintained on the central X drive. Hard copy files to be stored offsite for 5 years after which they will be securely destroyed.  Archived onsite for one year following success at the Part B MFPH examination, or 3 years following success at the Part A MFPH examination. Then offsite for 5 years after which they will be securely destroyed. | The historic record of training posts and examination results is to be maintained on the database indefinitely.  This period of 10 years covers a minimum of two revalidations from the completion of training. If they have been granted full registration, the GMC will have copies of the necessary references. Education files for training members is a record of an individual’s training and therefore no information should be destroyed until after they have received their CCT. Iron Mountain is to be used to archive all Education files till all the files are scanned in and electronically stored. |
| **Examinations**  Question papers  Examination answer scripts (Part A MFPH)  Examiner marking forms (Part B MFPH)  Examination results/marks  Examiner files | All examination question papers are to be kept indefinitely electronically. Hard copies to be destroyed within 1 month after examinations.  Answer scripts are to be kept onsite for one month after the release of results for the examination sitting to which they relate and for a further 2 years offsite after which they will be securely destroyed.  Marking forms to be kept onsite for 2 years and for a further 2 years offsite after which they will be securely destroyed.  All examination results and marks to be kept indefinitely electronically.  Examiner applications/ curriculum vitaes/ correspondence to be kept on site for 3 years following end of examiner term then securely destroyed. | Copies of question papers are to be retained in the appropriate folder of the Education & Training Department.  Examination marks to be retained in appropriate folders/databases of the Education & Training Department.  Unsuccessful examiner applications and the reasons for their rejection are also to be retained on site for three years and then securely destroyed. |

### Professional Standards

|  |  |  |
| --- | --- | --- |
| Professional Standards***:- Membership, AAC’s, CPD*** | | |
| ***DOCUMENTS*** | ***RETENTION PERIOD*** | ***REASON FOR RETENTION PERIOD & COMMENTS*** |
| General Correspondence | **5** years | Any correspondence relating to Fellows, Members and Trainees are to be kept electronically for 5 years after membership has ceased. Address changes/Yellow forms should be securely destroyed when updated by a new one. |
| Equal Opportunities Form, Curriculum Vitae & Examination certificates | **T**o be kept on members’ electronic record indefinitely | As this could be classified as sensitive data only the most recent/current copy should be kept. All previous copies to be returned to the member concerned or securely destroyed. |
| ALL paperwork relating to individual AACs i.e. job description, personal specification, draft advertisement, written approval from Faculty Advisor, list of Assessors  Faculty Assessors’ application forms i.e. application form, equal opportunities training qualification.  General AAC correspondence | **T**o be retained for 5 years.  **T**o be retained indefinitely.  **T**o be retained for 5 years. | Should be filed in the office for six months for quick reference.  After this time paperwork can be scanned and archived and kept for a total of 5 years and then securely destroyed. It is the responsibility of the employing body to keep a full record of the AAC itself.  Original acceptance and contact information even after retirement; this is for proof of attendance at Equal Opportunities Training.  To be scanned onto a CD on an annual basis and paper files securely destroyed within this time period. |
| Membership Elections and Admissions | **T**he default storage limit on MessageLabs is 3 years. | Dates of election are recorded on individual’s records indefinitely. The officers approve all elections via email. It therefore can be stored and archived on MessageLabs. |
| Nominations through Fellowship Committee | **T**his list will be kept electronically and kept indefinitely  **T**o be kept for 18 months before securely being destroyed. | A list of the Faculty medals, awards and prizes and the recipients of these in date order is kept electronically and is regularly updated.  All paper work relating to nominations |
| CPD annual returns  Application for Exemption  Audit submissions  CPD Co-Ordinator Committee | 5 years once retired.  Kept indefinitely  Scanned onto electronic record of the individual and kept indefinitely.  To be retained for 1 year | All agenda’s and minutes to show all decisions taken |
| Revalidation Appraisal Portfolios | Kept in a secure folder for 5 years – until the end of the cycle | The RO and any new ROs may need to access the information contained within the portfolio in order to make a recommendation or share information when an individual moves between designated bodies. |
| Revalidation RO Dashboard | Kept indefinitely in a secure folder | The RO may need to access the information contained within the dashboard in order to share information when an individual moves between designated bodies.  The Dashboard contains a summary of any concerns and the appraiser output statements. |
| Revalidation Prescribed connections | Kept indefinitely in a secure folder | The RO and any new ROs may need to share information when an individual moves between designated bodies. |
| Documentation for those no longer connected to FPH as a designated body | Kept indefinitely in a secure folder | The RO may need to access the information in order to share information when an individual moves between designated bodies. |
| Revalidation Queries Log | Kept for 5 years to auditing purposes |  |
| Revalidation email inbox | Kept for 5 years to auditing purposes | Contains revalidation queries and responses. |
| Letter from GMC regarding recommendations | Kept indefinitely in a secure folder | The RO may need to access the information contained within the dashboard in order to share information when an individual moves between designated bodies. |
|  |  |  |
|  |  |  |

1. http://www.soas.ac.uk/infocomp/dpa/policy/overview/ [↑](#footnote-ref-1)
2. <http://www.ico.gov.uk/tools_and_resources/glossary.aspx#s> [↑](#footnote-ref-2)