

The Faculty of Public Health (FPH) Data Protection Policy
Approved by the FPH Board on 28 February 2019

The UK Faculty of Public Health (FPH) is a membership organisation for nearly 4,000 public health professionals across the UK and around the world. We are also a registered charity. We exist to enable the advancement of knowledge and maintain the highest possible standard of professional competence. We act as an authoritative body for the purpose of consultation and advocacy in matters of educational or public interest concerning public health.

In order to satisfy operational and legal obligations FPH processes and maintains personal information about its staff, members and other individuals. FPH may require information about current, past and prospective employees, FPH members, suppliers and other individuals with whom it has business or with whom it communicates.

FPH fully endorses and adheres to the Data Protection Act 2018 which is the UK’s implementation of the General Data Protection Regulation (GDPR). The Data Protection Act 2018 (the 'Act' for purposes of this policy) was introduced in May and all FPH employees and other individuals who obtain, handle, process, disclose, transport and store personal data for FPH are expected to adhere to these principles.

The guiding principles of GDPR are as follows:

(a) – lawfulness, fairness and transparency

(b) – purpose limitation

(c) – data minimisation

(d) – accuracy

(e) – storage limitation

(f) – integrity and confidentiality

In more detail:

(a) data is processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’);

(b) is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).”

FPH has put in place appropriate organisational and management controls to ensure it meets its obligations to observe these principles. These are outlined in the FPH Data Protection Procedures and Guidance document and summarised below.

Main role definitions

* Processing is the act of obtaining, recording, holding or using personal data.
* Data subject is an individual who is the subject of personal data (a data subject must be alive).
* Data controller is a person or organisation that decides how personal data is processed.
* Data processor is any person or organisation that processes data on behalf of the data controller.

Subject Consent

FPH has identified the lawful purposes for which it collects data – this is known as the “legitimate interest”. Much of this data is required so that FPH can meet its contractual agreement with members/clients, and these requirements to process personal data are made known to all data subjects. We seek consent from data subjects to process personal data. If we collect any sensitive personal data, for example information about health, race or gender, express consent to process the data will be obtained.

Subject Access

FPH will ensure that the rights of individuals who are the subject of personal data held by FPH can be fully exercised. GDPR provides an individual with:

* The right to be informed
* The right of access
* The right to rectification
* The right to erasure
* The right to restrict processing
* The right to data portability
* The right to object
* Rights in relation to automated decision making and profiling.

This is subject to certain exemptions which are set out in the [ICO website](https://ico.org.uk/your-data-matters/your-right-of-access/). Any individual may make a subject access request to any FPH staff member. Although subject access requests may be made verbally, we would advise that a request may be dealt with more efficiently and effectively if it is made in writing. FPH implemented a revised Subject Access Request Policy in summer 2018.

Publication of FPH information

FPH will seek permission from individuals before transferring any personal data to a third party such as media and will make clear from the outset the nature of the query and the ways in which any information given can be used.

Information that is already in the public domain is exempt from the Act and includes for example information on staff or members contained within externally circulated publications such as the Annual Reports, Journal of Public Health and *Public Health Today*. (Publications may be hard copy or electronic.)

Disclosure of data

FPH will ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends and government bodies and in certain circumstances, the Police without prior notification.

Data security

FPH will ensure that personal data are kept securely and adequate precautions taken against physical loss or damage regardless of whether it is held in paper or electronic format.

Data retention and disposal

FPH will retain data only for the period of time required for processing in accordance with the Act and with other relevant laws. FPH will ensure that data is disposed of in a way that protects the rights and privacy of data subjects.

Employee supervision, awareness and training

FPH will:

* appoint someone with specific responsibility for data protection;
* ensure that everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
* describe clearly methods of handling personal information;
* arrange for appropriate training for everyone managing and handling personal information;
* supervise appropriately everyone managing and handling personal information;
* ensure that staff deal with queries about personal information promptly and courteously;
* conduct a regular review and audit of the way personal information is managed;
* assess and evaluate regularly methods of handling personal information.

FPH reserves the right to modify this policy at any stage. It will carry out regular assessments of compliance with the Data Protection Act 2018.

Designated Roles at FPH

FPH as an organisation is the Data Controller and thus ultimately responsible for legal compliance, this means that Chief Executive and the Trustees of FPH are responsible for ensuring that the Data Protection policy is adequate, correct and reviewed regularly.

The Director of Business Services is the FPH Data Protection Officer

For further information or for a copy of the FPH Data Protection Procedures and Guidance document please contact:

Dr James Gore, Chief Executive
Faculty of Public Health

4 St Andrew Place, London, UK, NW1 4LB
Email: jamesgore@fph.org.uk Telephone: +44(0) 20 3696 1462

**Document revised January 2019**

**Document revised by Mag Connolly, Director of Business Services**

**Next review date April 2019.**