Data Protection Policy

1. Purpose and Scope

This policy explains how the Faculty of Public Health (FPH) complies with the UK's Data Protection Act 2018. FPH is committed to data protection and individual's rights and obligations in relation to personal data as well as being transparent about how it collects and uses the personal data of its members and employees.

This policy applies to all personal data handled FPH.

The purpose of this policy is to ensure that FPH and the FPH staff team comply with the General Data Protection Regulation (GDPR) when processing personal data. This policy applies regardless of where the data is held.

This policy applies to all staff, whether permanent, temporary, contractors, consultants or secondees and includes Officers, Board of Trustees/Committee members and volunteers.

2. Data Protection Officer

FPH has appointed Kajol Kohar, as the Data Protection Officer (DPO). This person will hold responsibility for data protection compliance within FPH.

3. Definitions

Personal data is any information that relates to an individual who can be identified from that information.

The data controller exercises overall control over the purpose for which, and the manner in which, personal data are processed.

Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Special categories of personal data or sensitive personal data means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, genetics and biometric data.

Criminal records data means information about an individual's criminal offences and convictions, and information relating to criminal allegations and proceedings.

4. Data protection principles

FPH process personal data in accordance with the following data protection principles:

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) Data is kept accurate and up to date. Taking all reasonable steps to ensure that inaccurate or out of date personal data is erased or rectified without delay ('accuracy')
e) keeps personal data only for the period necessary and for the purposes for which it is processed
f) data is processes personal data in line with the data subject's rights
g) 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')."
h) FPH will not transfer data to countries outside the European Economic Area (EEA) without adequate protection i.e. without recognised statutory data protection equivalents.

FPH has put in place appropriate organisational and management controls to ensure it meets its obligations to observe these principles.

5. Legal Basis for processing personal or sensitive data

FPH will only process personal data if it can satisfy at least one of the following conditions in relation to that data:

a) **consent** – the data subject whom the personal data is about has consented to the processing contractual – processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract eg for an employment contract.

b) **legal obligation** – processing is necessary for compliance with a legal obligation protection of vital interests of a data subject – where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person

c) **public interest/official authority** – processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest

d) **legitimate interests** – processing is necessary for purposes of legitimate interests pursued by FPH or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

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/employees etc. and these requirements for processing 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, explicit consent to process the data will be obtained.

FPH will only process special category data or criminal records where:

a) The data subject has given explicit consent to the processing of the personal data for one or more specified purposes. For the consent to be explicit, the data subject must signify their agreement and there must be some statement or a clear affirmative action that signifies agreement to the processing of personal data relating to them

b) The information is required by law to process the data for employment purposes
c) The information is needed to protect the vital interests of the data subject or another, and consent cannot be given or reasonably sought.

FPH has a Data Retention Policy to ensure that personal data processed for any purpose(s) shall only be kept for as long as a business process requires or to fulfil legal obligations to record keeping, depending on which is the longest.

FPH will ensure that its processing activities are registered with the Information Commissioners Office (ICO).

FPH will make its Privacy Notice available on its website.

6. Individual Rights

As a data subject, individuals have a number of rights in relation to their personal data. 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 to 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.

To request any of the above, the individual should send a request to datacontroller@fph.org.uk

a) The Right to Access - Data Subject Access Requests (DSAR)

Individuals are entitled to access the information that FPH holds about them. This is known as the right to access.

If an individual makes a data subject access request (DSAR), FPH will comply with the relevant legislation:

- confirm whether any personal data is being processed
- provide a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
- provide a copy of the information comprising the data; and details of the source of the data (where this is available).

This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

If the individual wants additional copies, FPH may charge a fee that will be based on the administrative cost of providing the additional copies.

To make a data subject access request, the individual should complete the data subject access request form and send it to the Data Protection Officer at datacontroller@fph.org.uk. The DPO will act in accordance to FPHs Data Subject Access Request Policy.

7. Data security

FPH takes the security of personal data seriously and has internal policies and controls in place to protect personal data at rest or in transit against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by staff in the proper performance of their duties.

Where FPH engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, i.e. a data sharing agreement and/or under contractual agreement. Third party suppliers are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

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.)

8. International data transfers

FPH will not transfer personal data to countries outside the EEA unless there are suitable safeguards, and the country or territory can ensure an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

9. Impact assessments

Some of the processing that FPH carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, FPH will carry out a Data Privacy Impact Assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks to individuals and the measures that can be put in place to mitigate those risks.

10. 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.

11. Training

FPH provides information and training to all staff about their data protection responsibilities as part of the induction process and provides annua refresher training thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy and responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them

12. Breach of Policy

Failing to observe these requirements may amount to a disciplinary offence that will be dealt with under FPH's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or members' data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

The following policies, procedures and guidance should be used or referred to as necessary alongside this policy. All policies and templates are made available to staff on the central drive.

a) Data Retention Policy and Schedule.
b) Subject Access Request Policy and Form.
c) Data Protection and GDPR Guidance Handbook for Staff.
d) Privacy Notices.
e) Data Breach Notification Policy
f) Remote Access and Mobile Working Policy
g) Data Portability Policy
h) Data Sharing Agreement Process and Template
i) Data Protection Impact Assessment (DPIA) Policy and Template
j) Erasure Policy
k) Information Security Policy

13. Policy Review and Document History

This policy will be reviewed annually or when significant changes in data protection laws occur.

Last review date	March 2025
Last modification date (approved by FPH Board)	March 2025
Next review date	March 2026