

The Friends of Queen Mary's Hospital Data Retention Policy - May 2018

1. Introduction

This Policy sets out the obligations of The Friends of Queen Mary's Hospital, a charity registered in The United Kingdom under number 266438, whose registered office is at The Friends of Queen Mary's Hospital, Roehampton Lane, London SW15 5PN ("the Charity") regarding retention of personal data collected, held, and processed by the Charity in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

- a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
- b) When the data subject withdraws their consent;
- c) When the data subject objects to the processing of their personal data and the Charity has no overriding legitimate interest;
- d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);
- e) When the personal data has to be erased to comply with a legal obligation; or
- f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Charity for the purposes of running the said Charity, the periods for which that personal data is to be retained, the criteria for establishing and reviewing such periods, and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR, please refer to the Charity's Data Protection Policy.

2. Aims and Objectives

1. The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Charity complies fully with its obligations and the rights of data subjects under the GDPR.
2. In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Charity, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

1. This Policy applies to all personal data held by the Charity including data relating to Friends membership, bequests and donations volunteers, employees and Trustees of the Charity.
2. Personal data, as held by the Charity is stored in the following ways and in the following locations:
 - a) The Charity's servers, located at The Friends of Queen Mary's Hospital, Roehampton Lane, London SW15 5PN;
 - b) Computers permanently located in the Charity's premises at The Friends of Queen Mary's Hospital, Roehampton Lane, London SW15 5PN;
 - c) Laptop computers and other mobile devices provided by the Charity to its employees;
 - d) Computers and mobile devices owned by employees;
 - e) Physical records stored at The Friends of Queen Mary's Hospital, Roehampton Lane, London SW15 5PN.

4. Data Subject Rights and Data Integrity

All personal data held by the Charity is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Charity's Data Protection Policy.

1. Data subjects are kept fully informed of their rights, of what personal data the Charity holds about them, how that personal data is used as set out in the Charity's Data Protection Policy, and how long the Charity will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).
2. Data subjects are given control over their personal data held by the Charity including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Charity's use of their personal data and further rights relating to automated decision-making and profiling as set out in the Charity's Data Protection Policy.

5. Technical and Organisational Data Security Measures

1. The following technical measures are in place within the Charity to protect the

security of personal data. Please refer to Parts 19 to 23 of the Charity's Data Protection Policy for further details:

- a) All emails containing personal data must be marked "confidential";
- b) Personal data may only be transmitted over secure networks;
- c) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;
- d) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;
- e) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;
- f) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient;
- g) All personal data transferred physically should be transferred in a suitable container marked "confidential";
- h) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from.
- i) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;
- j) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Charity or not, without authorisation;
- k) Personal data must be handled with care at all times and should not be left unattended or on view;
- l) Computers used to view personal data must always be locked before being left unattended;
- m) No personal data should be stored on any mobile device, whether such device belongs to the Charity or otherwise without the formal written approval of the Executive Chairman and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;
- n) All personal data stored electronically should be backed up regularly with backups stored offsite;
- o) All electronic copies of personal data should be stored securely using passwords;
- p) All passwords used to protect personal data should be changed regularly and should must be secure;
- q) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- r) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;
- s) No software may be installed on any Company-owned computer or device without approval; and
- t) Where personal data held by the Charity is used for marketing purposes, it shall be the responsibility of the Secretary to ensure that the appropriate consent is obtained and that no data subjects have opted out.

2. The following organisational measures are in place within the Charity to protect the security of personal data. Please refer to the Charity's Data Protection Policy for further details:
 - a) All employees and other parties working on behalf of the Charity shall be made fully aware of both their individual responsibilities and the Charity's responsibilities under the GDPR and under the Charity's Data Protection Policy;
 - b) Only employees and other parties working on behalf of the Charity that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Charity;
 - c) All employees and other parties working on behalf of the Charity handling personal data will be appropriately trained to do so;
 - d) All employees and other parties working on behalf of the Charity handling personal data will be appropriately supervised;
 - e) All employees and other parties working on behalf of the Charity handling personal data should exercise care and caution when discussing any work relating to personal data at all times;
 - f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
 - g) The performance of those employees and other parties working on behalf of the Charity handling personal data shall be regularly evaluated and reviewed;
 - h) All employees and other parties working on behalf of the Charity handling personal data will be bound by contract to comply with the GDPR and the Charity's Data Protection Policy;
 - i) All agents, contractors, or other parties working on behalf of the Charity handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Charity arising out of the GDPR and the Charity's Data Protection Policy;
 - j) Where any agent, contractor or other party working on behalf of the Charity handling personal data fails in their obligations under the GDPR and/or the Charity's Data Protection Policy, that party shall indemnify and hold harmless the Charity against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

1. Personal data stored electronically (including any and all backups thereof) shall be deleted using the delete function contained within the software that is being used for the purposes of storing the data.
2. Personal data stored in hardcopy form shall be shredded or disposed of by a recognised secure disposal service.

7. Data Retention

1. As stated above, and as required by law, the Charity shall not retain any personal data for any longer than is necessary in light of the purpose(s) for

which that data is collected, held, and processed.

2. Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.
3. When establishing and/or reviewing retention periods, the following shall be taken into account:
 - a) The objectives and requirements of the Charity;
 - b) The type of personal data in question;
 - c) The purpose(s) for which the data in question is collected, held, and processed;
 - d) The Charity's legal basis for collecting, holding, and processing that data;
 - e) The category or categories of data subject to whom the data relates.
4. If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.
5. Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Charity to do so (whether in response to a request by a data subject or otherwise).

Data Ref.	Type of Data	Purpose of Data	Review Period	Retention Period or Criteria	Comments
Friends	Name, address, email, phone number, subscription due date, gift aid consent, method of payment, method of contact	To manage the relationship with Friends including annual subscription mailing, funding updates and annual report	Annually	General data to be retained for 60 days following expiry of membership Gift Aid records to be retained for six years plus current year	
Donors	Name, address, email, phone number, gift aid consent method of payment, amount, payment details, specific requests for bequest	To record details of one off bequests for recognition and thanks, PR and Marketing, annual account reporting and informing the Friends Committee	Annually	General data to be retained for 60 days following expiry of membership Gift Aid records to be retained for six years plus current year	

Volunteers including Pets as therapy	Name, address, email, phone number, age, gender, ethnicity, nationality, religion, interview notes, CV, assessments	To manage the volunteers	Annually	60 days from cessation of role	
Employees	Name, address, email, phone number, age, gender, ethnicity, nationality, religion, interview notes, CV, assessments, contract details, payroll and HMRC details,	To manage employer/employee relationship	Annually	Six years plus balance of current year	
General Committee members	Name, address, email, phone	Management of day to day Committee business	Annually	30 days from resignation from the Committee	
Committee members who are recognised officials	Name, address, email, phone number, passport number and expiry date, date of birth, National Insurance number	Retained as required for the Charity commission	Annually	30 days from resignation from office	
Traders	Name, address, email, phone number, Insurance details, signed terms and conditions agreement	To manage the working relationship with the table top traders and other traders operating in Queen Mary's on behalf of the Friends	Annually	Six years plus remainder of current year	

8. Roles and Responsibilities

1. The Charity's Data Protection Officer is Charles Shiplee who is a member of the Friends Committee.
2. The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Charity's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.
3. The Data Protection Officer shall be directly responsible for ensuring compliance with the above data retention periods throughout the Charity. Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

9. Implementation of Policy

This Policy shall be deemed effective as of 1st May 2018 No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Linda Lamb
Position: Chair of Friends Committee
Date: 25th May 2018
Due for Review by: 1st May 2019
Signature: A signed copy to available to view at the Friends office