Peterborough & District Family History Society
DATA PROTECTION POLICY

Key details

Policy prepared by:	Colin Ashworth on 9 April 2018
Approved by the committee on:	[Enter DATE]
Policy became operational on:	[Enter DATE]
Next review date:	[April 30th 2019]

Key Personnel

Data Controller

The P&DFHS Committee	c/o secretarypdfhs@gmail.com	
Data Processors		
The Information Manager	Colin Ashworth	editorandmembership@gmail.com
The Journal Editor	Colin Ashworth	editorandmembership@gmail.com
The Membership Secretary	Colin Ashworth	editorandmembership@gmail.com
The Secretary	Helen Tovey	secretarypdfhs@gmail.com
The Treasurer	(*Kevin Terrington)*	treasurerpdfhs@gmail.com
The Webmaster	Alan Johnson	alanpdfhs@btinternet.com
The Archivist	Alan Johnson	alanpdfhs@btinternet.com

This Policy should be read in conjunction with the society's **Privacy Statement** which outlines some of the ways in which aspects of the policy can be implemented.

INTRODUCTION

Peterborough & District Family History Society (P&DFHS) needs to gather and use certain information about individuals who will, in the main, be paying or honorary members of the society. The data of others may be sent to the society by non-members making an initial approach via any P&DFHS post-holder. We may also hold information about speakers, suppliers and business contacts (such as our printer), magazines, our website hosting service and other people with whom the society has a relationship, or may need to contact.

Why this policy exists

This policy describes how personal data must be collected, handled and stored to meet the society's data protection standards and it ensures that the P&DFHS

- Complies with data protection law and follows good practice
- Protects the rights of post holders, members, suppliers and other contacts
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Society GDPR Documents

The society has produced the following documents

- PDFHS GDPR Data Protection Policy.doc {Which is this current document}
- PDFHS GDPR Consent Agreement (All).doc
- PDFHS GDPR Consent Agreement (Committee).doc
- PDFHS GDPR Privacy Statement.doc

Data protection law

- The General Data Protection Regulation (GDPR), which replaced the Data Protection Act 1998 in May 2018, describes how organisations - including P&DFHS - must collect, handle and store personal information.
- These rules apply regardless of whether data is stored electronically, on paper or on other materials.
- To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

PEOPLE, RISKS & RESPONSIBILITIES

Policy scope

This policy applies to:

- The committee of the P&DFHS
- All post holders and volunteers of P&DFHS
- All contractors, suppliers and other people working on behalf of P&DFHS as described in the introduction
- It applies to all data that the society holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include:
    a) Names of individuals (*Members, Speakers, Non-members who buy CDs of our Archives, Names written in the meeting attendance book*) and their:
        i. Postal addresses
        ii. Email addresses
        iii. Telephone numbers
    b) Bank details of members paying by Standing Order
    c) Any other information relating to identifiable individuals
    d) Gift Aid information

Data protection risks

This policy helps to protect the P&DFHS from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the society uses data relating to them.
- Reputational damage. For instance, the society could suffer if hackers successfully gained access to sensitive data.

Responsibilities

- The committee is ultimately responsible for ensuring that the P&DFHS meets its legal obligations
- Everyone who works for or with P&DFHS has some responsibility for ensuring data is collected, stored and handled appropriately.
- Everyone who processes personal data must ensure that it is handled and processed in line with this policy and data protection principles.
- The following people have key areas of responsibility:

The Information Manager has responsibility for:

a) Keeping the committee updated about data protection responsibilities, risks and issues.
b) Reviewing all data protection procedures and related policies, in line with an agreed schedule.
c) Arranging data protection training and advice for the people covered by this policy.
d) Handling data protection questions from the committee and anyone else covered by this policy.
e) Dealing with requests from individuals concerning the data P&DFHS holds about them (also called **'subject access requests'**)
f) Checking and approving any contracts or agreements with third parties that may handle the society's sensitive data, although this will be rare.

Other Data Processors (as listed on page 1) have these responsibilities:

a) To ensure that the personal IT and paper-based systems, services and equipment used for storing data meet acceptable security standards.
b) To perform regular checks and scans to ensure security hardware and software is functioning properly. (Mainly using Anti-Virus Software and utilities such as Malwarebytes, or Adaware software)
c) To evaluate any third-party services the society may consider using to store or process data; for instance, cloud computing services or web hosting services.
d) Using data protection statements – approved by the committee – to attach to communications such as emails and letters.
e) Addressing any data protection queries from journalists or media outlets like newspapers.
f) Where necessary, working with other post-holders or committee members to ensure marketing initiatives abide by data protection principles.

GUIDELINES

General Guidelines

a) The P&DFHS will provide guidance to all committee members to help them understand their responsibilities when handling data.
b) The only people able to access data covered by this policy should be those who need it for their work on behalf of the society. These will normally be Membership Secretary, Journal Editor, Treasurer and Secretary.
c) The Journal Editor will liaise with the Information Manager (when the posts are not held by the same individual) to ensure that the data concerning committee members, when published in printed form, is only that for which consent has been given.
    - The society's current policy re electronic journals is not to include any individual committee member information except contact details for the Journal editor.

d) Data Processors should request help from the Information Manager if they are unsure about any aspect of data protection. They should keep all data secure, by taking the sensible precautions contained in this document.
e) Personal data should not be disclosed to unauthorised people, either within the society or externally.
f) Data should be regularly reviewed and updated if it is found to be out of date. Members should know how to advise Processors of any changes which need to be made.

Data storage

These guidelines describe how and where data should be safely stored. It should be remembered that although "membership data" will usually only need to be held and accessed by the Secretary, Membership Secretary and Treasurer, there may be other data relating to identifiable living people in the archives and thus the following points apply to those INDIVIDUAL records as well.

The Information Manager will ensure that the Data Processors store data safely and report back to the Data Controller (the committee) at regular intervals. All guidelines also apply to data which was originally supplied on paper or that which is usually stored electronically but has been printed out for some reason.

When data is stored electronically:

1. It must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
2. Strong passwords should be used by Data Processors and they should never be shared: ideally they should be changed regularly.
3. If data is stored on removable media (External HDD, CD, DVD or memory stick), these should be kept locked away securely when not being used.
4. Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services and/or website hosting services.
5. Data should be backed up frequently by Processors. Whilst a new backup should ideally replace an older copy, the Grandfather-Father-Son protocol is an appropriate one to employ: a new backup should replace the oldest of the three copies. Numerous copies of data sets should not be retained unless they are being Archived for genuine reasons. Data will be held in as few places as necessary. Data Processors should not create any unnecessary additional data sets.
6. All servers and computers containing data should be protected by approved security software and a firewall.

When data is sent electronically from one Processor to another:

1. It should be both encrypted and password protected and the means to access it be known to the receiver.
2. Clearly, passwords should not be sent at the same time as the actual data.
3. Once the data has been received, the password used for delivery should ideally be changed to another by the recipient.

When data is stored on paper:

1. It should be kept in a secure place where unauthorised people cannot see it.
2. When not in use, the paper or files should be kept in a locked drawer or filing cabinet.
3. Data Processors should make sure paper and printouts are not left where unauthorised people could see them, such as on a printer.

Data use

Personal data is of no value to P&DFHS unless the society can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.

a) When working with personal data, Data Processors should ensure the screens of their computers are always locked when left unattended.
b) Personal data should not be shared informally.
c) Bulk emails to members should be sent BCC (Blind copied). They will not normally need to be encrypted.
d) Committee members will need to consent to discussion emails being sent with visible addresses (i.e. Reply All). Committee members who prefer not to receive such emails in their personal Inbox may wish to set up a dedicated email account for society business.
e) Personal data should never be transferred outside of the European Economic Area. Electronic (PDF) Journal sent overseas will have the back cover (with committee details) removed.

Data accuracy

a) The law requires the society to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort society should put into ensuring its accuracy.
b) The Membership Secretary will have the most up to date data. It will be checked by the Membership Secretary on a quarterly basis at each Journal posting.
c) All Data Processors should take reasonable steps to ensure that the Membership Secretary has data which are accurate and as up to date as possible by informing the Membership Secretary of any changes they discover (e.g. A member mentions a change at a meeting)
d) The society will make it easy for data subjects (especially members) to update the information which the society holds about them. The method is outlined on the Privacy Statement.
e) Data should be updated as soon as inaccuracies are discovered. For instance, if a member can no longer be reached on their stored telephone number, it should be removed from the database.
f) Members will be regularly reminded to help the society keep their details up to date.

Date retention and deletion

Reasons to retain data (including paper copies) include:

1. An individual is a current society member.
2. Details have – with consent – already been included (for committee members) in paper copies of the Journal. {Electronic (pdf) versions of the publication also form part of the society's historical archive and are stored in 'members only' area of the website but with the back cover removed.}
3. Backups and Archives are different.
    a. **Backups** exist in case information is accidentally destroyed. Backups should cover all information, but each one only needs to be kept for a short time: essentially however long it will take the organisation to discover the destruction. Since they are only needed when something goes wrong, access to them can be tightly limited. Backups should use the grandparent-parent-child principle i.e. when a new backup created then the current "Grandparent" file becomes a "Great-Grandparent file" and is erased in accordance with the society processes described under Data Storage.
    b. **Archives**, involve long-term storage of an organisation's history and other information pertinent to the Constitutional Aims and Objectives. They should only contain the selected subset of information which constitutes the society's history

and which meets those Constitutional Aims and Objectives satisfactorily. Organisations intend that their archives will be used, so should store them with indexes and structures that make that easy to locate.

4. Memberships are due for renewal on April 1st each year. If a member has not renewed by 15th May they will be sent an email (or letter for non email users) informing them that they have been deemed to be non-members. They will have 10 days to contact the society if they wish to revive and retain their member status. However, if no reply is received then all data will be deleted from society records, except for any required for statutory purposes, to enable the society to comply with Data Protection requirements.
5. Members who rejoin the society once their membership has lapsed will be given new membership numbers. This removes the need to retain any data pertaining to previous periods of membership (such as old membership numbers).
6. Even though a current member requests that data should no longer be processed, or a lapsed member's data is scheduled for deletion, some of their personal data may need to be retained to meet statutory requirements e.g. Gift Aid information which is retained for 7 years. The Treasurer and Membership Secretary should liaise closely in these circumstances and advise the data subject of the information retained and why.

Reasons to delete data (including paper copies) include:

1. A member leaves the society. An individual may allow their membership to expire or request that it ceases immediately. See 6 above.
2. A member dies.
3. A member specifically requests that their data is not retained. (At any time, a member may request that their data is not processed but it may be retained for the duration of their membership). If a member requests that their data is not retained the portion of it required to comply with Statutory Requirements will be stored and the member informed.
4. The society is wound up.

SUBJECT ACCESS REQUESTS

This section deals with the entitlements of individuals who are the subject of personal data held by P&DFHS.

Requests from data subjects

a) Individuals may ask what information the society holds about them and why. If an individual contacts the society requesting this information, this is called a "subject access request".
b) They should know how to gain access to their information.
c) They should know how to keep it up to date.
d) Individuals are entitled to be informed how the society is meeting its data protection obligations.
e) They should know that they may receive a copy of the information free of charge. (However, a 'reasonable fee' may be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive.)
f) Subject access requests from individuals should preferably be made by email, addressed to the Membership Secretary.
g) The Membership Secretary on behalf of the Data Controller will aim to provide the relevant data within 14 days.
h) The Membership Secretary on behalf of the Data Controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

a) In certain circumstances, the Data Protection Regulations allow personal data to be disclosed to law enforcement agencies or other statutory bodies (e.g. HMRC) without the consent of the data subject.
b) Under these circumstances, P&DFHS will disclose requested data. However, the Membership Secretary will ensure the request is legitimate, seeking assistance from the committee (and possibly from a legal adviser) where necessary.

Providing information

The P&DFHS aims to ensure that individuals are aware that their data is being processed, and that they understand:

a) How the data is being used
b) How to exercise their rights

To these ends, the society has a privacy statement, setting out how data relating to individuals is used. This is available on request. Both the privacy policy statement and this data protection policy statement is available on the society's website at http://www.peterborofhs.org.uk/Data-Protection-Information.php

***** DOCUMENT ENDS *****

This document is based upon a template downloaded from IT Donut (www.itdonut.co.uk) who kindly made it available to their website visitors.