Abbeyfield Oxford Society Ltd
Brian Lewis House
80 St Clement's Street
Oxford
OX4 1AW

DATA CONFIDENTIALITY, PRIVACY, PROTECTION & RETENTION POLICY

1. Context, aims & objectives of this policy

Our Society holds data for regulatory and management purposes. We recognise our obligations regarding confidentiality and our legal obligation to safeguard the data we hold and will respect and protect the privacy of our residents, staff, trustees, volunteers and member data by keeping this secure and confidential. We will only use personal information held about others, whether employees, members, volunteers or residents, for the purposes for which it was provided and only disclose it to those others who are entitled to see it for the same purposes. A key objective of this Policy is to help ensure that everyone who views or handles data and information in any format as part of their duties or employment with us meets these requirements. Particular care must be taken to avoid accidental disclosure of information.
An appendix also details how long we keep information in various categories.

What does this mean for me?

Unless specifically authorised by our Board to do so as part of your duties as an employee, trustee or volunteer, you may not use or disclose to any other person during or after working for or with our Society, any confidential documents, facts, information or trade secrets relating to the business or affairs of the Society or its employees, trustees, members or volunteers which come to your knowledge during your work with us. More detail is included in the Statement which forms part of this policy.

Similarly, you must not make or keep any copies of electronic or paper documents or extracts that come into your possession through your work with us other than for the purpose and in the course of your duties with us.

On termination of your involvement in any capacity with our Society, you must not take with you or keep any information about our residents, sales, suppliers, whether papers, charts, bulletins, reports, drawings, blueprints, models or any copies or extracts of these. Any and all such items belong to us and you must surrender them to us or destroy them.

2. Digital devices and content

The same principles apply to digital information. Smart phones and tablets can now store and transmit large quantities of data. Their use as a telephone is a small part of their function.
Inevitably trustees, volunteers and staff will use their own equipment for both their personal and work or volunteering roles. The same attention to data protection issues is needed when using such devices, whether Society or personally owned equipment which may receive, access, or store data.
In particular, access to the device must be password or e.g. fingerprint protected.
Mobile phones (including smart phones) tablets, computers and other equipment provided to our staff or volunteers for company use may only be used for that purpose. Costs associated with the

use of company supplied items will be reimbursed through the expenses system, as will calls for company business made on personally owned equipment (in which case detailed records need to be kept).

Devices which we provide remain our property. The user agrees to the following responsibilities:

- To be accountable for the device and its use until it is returned (Unauthorised transfer of devices is not allowed)
- To exercise reasonable care for the device, avoiding damage or loss.
- To use devices safely (see below)
- Not to use company phones for personal calls other than in exceptional circumstances. To advise if the company equipment is lost, stolen or damaged.
- To return equipment in good condition and any batteries, chargers etc. when required.

At the time of publication, the only such devices we supply are the laptop and desktop computers used by the House Manager and Administration Manager.

Social Media

If using social media the confidentiality and data protection rules described in this policy must be observed on any matters relating to our Society in general and our residents, staff and volunteers in particular, and controversial opinions should be avoided. The trustees are responsible for publication through any channel, including social media.

4. Guidelines for personal data

Staff and volunteers who process personal data must comply with the following conditions

- There must be a clear and foreseeable need for all personal data collected.
- Where specific personal information is sought from an individual, the individual should be informed as to the purposes for which that data will be processed.
- Personal data obtained for a specified purpose should not be processed for another purpose without the individual's consent (e.g. Where managers use pre-existing personal data to create their own systems, they should inform the individuals whose data is being used).
- Any personal data processed should be accurate, up to date, relevant, and not excessive for the purpose for which it is collected.
- Employees must be aware of how the data will be used.

5. Protection, Security and Retention of Information

We will ensure that appropriate technical and organisational measures are taken to safeguard personal data. Computer files containing personal data must be password protected, and our Society limits the number of people who will have access to centrally held data. Personal data should not be retained for longer than is necessary, and information will only be retained where there is a genuine business need to do so.

Retention periods for various categories of information are detailed in an Appendix to this policy. We will not keep information where there is only a small chance it may prove useful in the future.

Individuals have a personal responsibility to ensure that any personal or sensitive information to which they have access or come into contact during their work with us is protected from

unauthorised access and disclosure. This applies equally to data relating to residents, employees, trustees, volunteers and members, and to individuals outside our Society.

In particular, you and others must observe the following rules:

- Electronic storage of personal or sensitive material should be password protected.
- Paper copies of personal data must be held in designated secure cabinets or boxes, or securely destroyed immediately after use.
- Information should be labelled as 'Personal – Addressee Only'.
- Only disclose personal information to authorised colleagues. Take care not to do so accidentally, e.g. by being seen, overheard or mentioned to family or friends.
  It is good practice to anonymise data by use, e.g. of initials rather than names.
- All requests for information relating to an individual should be passed via the responsible person
- Particular care must be taken when exchanging information within Abbeyfield, or with third parties. Confidential information should only be sent electronically if the recipient has a secure network or comparable arrangements. Fax should not be used, nor should confidential information be printed in an open office. Ensure that any third party to whom the data is disclosed will keep the information secure and comply fully with the GDPR.
- Trustees and Volunteers receiving emails relating to Society business must protect these from access by others. Do not use an email account which can be viewed or shared with others.
- E-mails containing names and e-mail addresses of other individuals must not be forwarded outside the Society without their agreement.
- Information must not be used for purposes other than that for which it was intended
- If records are taken off-site, only necessary parts should be taken, and security measures should be taken to protect devices carrying it
- Paper-based documents removed from records must be confidentially destroyed.

Please be aware that disclosure of information in contravention of this Policy will be treated as a disciplinary offence, and further that under the GDPR individuals can be prosecuted or dismissed for improper use or unauthorised disclosure of such data.

6. General Data Protection Regulations (GDPR))

This and the following sections provide more detailed information for those responsible for managing and handling data. From 25th May 2018, provisions of the GDPR (previously the Data Protection Act) apply to records kept in files on computer and in some other formats.
We will follow the spirit of these provisions for all of our records to ensure we conform to these regulations.

6.1 **GDPR**

A self-assessment for our Society of GDPR requirements based upon the on-line Data Protection Toolkit provided by the Information Commissioners Office is included as an appendix to this policy. The steps needing to be taken to meet the criteria are also appended.

6.2 **Data Security and Protection Principles**

6.2.1 GDPR principles reiterate those described in Section 5 above, with the following definitions:

a) Personal Data is defined as data which relates to a living individual who can be identified from the data or from a combination of that data with other information in their possession, or likely

to come into the possession of the holder. Note that data does not have to be private or sensitive to constitute personal data and includes information such as names, addresses and telephone numbers. Personal data can cover both facts and opinions that are held about an individual. It also includes information regarding our Society's intentions towards the individual.
Data relates to any information held on a computer (including e-mails) or manually held paper records that have been stored in a structured way so that information can be found easily.

b) Sensitive Personal Data is defined as information about an individual's racial or ethnic origin, religious beliefs or other beliefs of a similar nature; trade union membership/non-membership; physical or mental health or condition; disability, sexual orientation, gender identity, crimes or alleged criminal offences or any proceedings for an offence or alleged offence.

Also, as mentioned above, disclosure of personal information outside our Society will normally only be made with the informed consent of the individual concerned. Exceptionally, we may need to do so, for example:

- To comply with the law (e.g. Police, Inland Revenue, Council Tax Registration Officer) or a court order.
- Where there is a clear health or safety risk or evidence of fraud.
- In connection with court proceedings or statutory action to enforce compliance with tenancy conditions (e.g. Applications for possession or for payment of HB direct).
- To provide the name, address and contact number of a resident to contractors or other agents providing services on the association's behalf.
- Anonymously for valid statistical or research purposes, provided it is not possible to identify the individuals to whom the information relates.

6.2.2 As Registered data users, we will comply with the following Data Protection Principles:

- Personal data must be obtained and processed fairly and lawfully.
- Personal data must only be held for the lawful purposes which are set out in our registry entry.
- Personal data must only be used for the purposes for which it was collected and it may only be disclosed to those people described in the register entry.
- Personal data must be adequate, relevant and not excessive in relation to the purpose for which it is held.
- Personal data must be accurate and up to date.
- Personal data must not be kept longer than is necessary for the registered purpose.
- Personal data must be accessible to the individual concerned, who has the right to have inaccurate information about themselves corrected or erased.
- Adequate security measures must be taken against unauthorised access, alteration, disclosure or accidental loss or destruction.

6.2.3 More specifically, our self-assessment and compliance with the security and protection principles mentioned above is based upon the following set of operational procedures and requirements.

Our registered "Data Controller" is The Abbeyfield Oxford Society Ltd.
Our nominated protection lead / information officer is the Administration Manager

Personal data which we currently hold includes the following:

- Personal Files and information held in paper format &/or on a computer
- List of names and addresses whether on spreadsheets or paper
- List of names and home telephone numbers
- Paper or computer based employee files containing employment records
- Training Records – including personal development plans
- Performance records
- Information received from third party benefits' providers regarding benefits choices e.g. pensions
- References provided to, or received from, external sources
- Management audit documentation
- Computer files holding the names of individuals
- Emails which mention an individual's name (note that there is regular email traffic between Trustees/Volunteers using their personal email addresses, and to a lesser extent staff). Care is taken not to include identifiable names (e.g. Resident X) should any content be of a personal nature.

This list is not exhaustive and may be subject to change.

Our Society's confidential data which is stored in computerised form is presently held on a PC located in the administration office, password protected, turned on and used only for company business and normally held by the Administration Manager (or a nominated individual when absent). The House Manager has a company laptop, password protected, turned on and used only for company business.
Such data is regularly backed up externally every day.
Non-confidential data company data (e.g. Our Policies) can be accessed via our network.
We have our own website, which holds no personal or business confidential information

Apart from banking records, external providers with access to confidential data are the Accounting firm which also handles payroll on our behalf and Careline who provide emergency assistance to residents out of hours. We have an appropriate confidentiality agreement with them both.

Confidential data or important items stored in paper form are held in securely locked cabinets (e.g. historical files) or secure boxes (e.g. current resident support, needs and risk assessment forms) accessible only to those authorised staff and volunteers involved.
To ensure fairness, openness and accuracy, in general items containing personal information relating to staff, residents or volunteers were either copied and given to them or seen and signed at the time it was created.
We have timely systems in place to review, update and/or delete out of date and expired information.
We do not use any externally supplied confidential data, e.g. for fundraising purposes.

All residents, staff and volunteers have access to all of our policies, either electronically or in paper format held at each house. It is a responsibility of both staff and volunteers to be familiar and comply with the contents of this policy (and others as designated).
Whilst the contents of this policy are not contractual, following appropriate consultation, we reserve the right to amend it without compensation.

d) More generally, the purposes for which we may hold and process an individual's personal data are as follows:

In relation to employment, including but not limited to:-
administering and maintaining personnel records; paying and reviewing salary and other remuneration and benefits; providing and administering benefits (including if relevant pension, life assurance and medical insurance); undertaking performance appraisals and reviews, including talent review and succession planning; dealing with performance, disciplinary, harassment and bullying, and grievance proceedings; providing references and information to future employers, and, if necessary, governmental bodies for social security and other purposes, e.g. The Inland Revenue and the Contributions Agency; providing information to future "purchasers" should the business of the Society be closed or transferred.

Similarly in relation to trustees, volunteers and self-employed workers in relation to their work with us, including (but not limited to) administering and maintaining records of work undertaken and expenses or remuneration payable, we may hold personal data including name, address, telephone number and emergency contact, bank account details and national insurance numbers, paper or computer based files containing job content and training records, information provided to, or received from, external sources and information contained on e-mail which mentions the individual's name. This list is not exhaustive and is subject to change.

In relation to Sensitive Personal Data, our Society may process

- Racial or ethnic origin for statistical monitoring purposes, in accordance with the Commission on Racial Equality guidelines.
- data on an individual's health for the purposes of maintaining sickness or other absence records*, and taking decisions as to an individual's fitness for work and entitlement to related benefits
- Information on criminal or alleged criminal offences in order to determine suitability for continued employment, where appropriate.

*Details of work related injuries or illnesses will be reported in accordance with legal requirements.

Sensitive personal data may also be processed, in accordance with data protection legislation, to exercise or perform a right or obligation conferred or imposed on us by law in connection with employment, legal proceedings or for the purpose of obtaining legal advice, or for administration of justice.

7. Rights of Access – Formal and Informal Requests

An individual may make an informal request to view a file that is held on him or her. If the individual requests to see his/her Personal file, it is important to ensure that he or she is only interested in viewing this file, rather than any other information held on him/her. If this is the case, a suitable time should be arranged for the individual to view his/her file, and to take copies of any documents contained within the file.

Requests by an ex-employee or other individual who has had any dealings with our Society should always be considered as a formal request. An individual is entitled

- to be told whether anyone in the Society is holding any of his/her personal data
- if so, to be given a description of the personal data held, the purposes for which the data is being processed and those to whom the information is/has or may be disclosed.

To make a formal request for access to all information held on an individual by the Society

- The individual should be advised to put a request in writing to our Administration Manager . There will be no charge for this unless the request is unfounded, excessive or repetitive in which case we reserve the right to charge a reasonable fee.
- Our Administration Manager will check to ensure that the individual is who he/she claims to be, validate his/her right to gain access to the data and consider the appropriateness of the request in line with the GDPR provisions.
- Our Administration Manager will contact the appropriate individuals within our Society and, where appropriate, any external organisations, and request access to or copies of all information held on that individual within any system or manual file (e.g. printouts of computer held records, copies of paper-based records).
- The individual will receive a response from the society within 30 days.

In some circumstances it may be appropriate for our Administration Manager to agree an appropriate time for the individual to review the information held on file, and take copies of documents, as appropriate. Where appropriate, any inaccuracies will subsequently be amended.

8. Disclosure of information relating to another person (an additional data subject)

Where documentation relating to an individual also discloses information relating to another person (an 'additional data subject'), this will also be the additional data subject's personal data.

The following steps must be followed when deciding whether to disclose data in these circumstances

- Try to get the additional data subject's consent to disclose this information. If consent is given, then the information should be disclosed.
- If consent is refused, but the feedback can be edited to remove all information which would identify the additional data subject, then the edited version should be disclosed.

Where consent has been refused (or cannot be obtained because the additional data subject has left our Society and cannot be traced), and it is not possible to 'anonymise' the information, we will need to decide if it is reasonable to disclose the data in any event. This will need to consider

- was the additional data subject aware when they wrote the document that it could possibly be released?
- any reasons given by the additional data subject for refusing consent to it being disclosed, whether releasing the information could be damaging to the additional data subject andwhat impact the documentation has, or might have in future, on actions or decisions relating to the individual.
- whether the feedback includes facts which the individual ought to be made aware of because he/she may dispute them andthe fact that greater protection must be given to information about someone's private life than information given in a business capacity.

9. Exemptions from Disclosure

We are entitled to refuse to disclose information in the following circumstances

- Confidential references given, or to be given by us
- References supplied to us, unless the provider has consented, or disclosure is otherwise reasonable in the circumstances
- Personal data processed for the purposes of management forecasting or planning, if disclosure would prejudice the conduct of the business
- Records of the employer's intention in connection with negotiations with the individual, if disclosure might prejudice those negotiations

10. Disclosure of information without informing the data subject

We are not required to notify an individual prior to disclosing informationabout them in the following circumstances

- Various exemptions for certain crime and taxation purposes, where compliance with the provision would be likely to prejudice the crime/taxation purpose.
- Where disclosure is required by law (e.g. requests from Inland Revenue, Child Support Agency, Benefits Agency, Department of Work and Pensions, Financial Services Authority) or a court order.

Where such disclosure is required and where practicablewe will seek to obtain the request in writing and also establish the identity and authority of the person making the request for disclosure.

If someone maintains that we have a legal obligation to disclose, ensure the request is received in writing, spelling out the basis on which legal obligation is asserted. Check the assertion is valid before disclosing. Make a copy available to the individual, and give him/her a chance to check the accuracy.

Keep a record of who made the disclosure;who authorised the disclosure;the person requesting the disclosure;the reasons for the disclosurethe information disclosed; andthe date and time of the disclosure.

In an emergency, generally in life and death situations, the request should be made in writing, if possible, and the disclosure should be made by the Administration Manager

The individual should be informed that the disclosure has been made if practicable.

11. Publication of information relating to individuals

No information should be published regarding individuals unless the individual has consented OR publication would be expected, the individual is informed in advance, their reasonable objections are respected and the information is not intrusive.

12. Appendices

The following are appended to this policy

Confidentiality & Privacy Policy Statement

Self Assessment of GDPR requirements

Document Retention and Disposal

13. Changes since last version

This generic policy has been prepared for use by member societies.

It combines several separate polices and new requirements relating to GDPR so that both format and content have been changed significantly compared to the original TAS equivalents.

APPENDIX: - **CONFIDENTIALITY AND PRIVACY POLICY STATEMENT**

Our overriding aim is to protect and promote the best interests of individuals and of the Society, and any question should be answered by reference to this principle. The Society, its staff and trustees will: -

- Treat all personal and sensitive organisational information as confidential to the Society;
- Comply with the law regarding the protection and disclosure of information;
- Not disclose personal information without the prior informed consent of the individual concerned, except in the circumstances outlined below in the section on disclosure;
- Not gain or attempt to gain access to information they are not authorised to have.

All personal information relating to residents, applicants, staff and trustees that is not a matter of public record will be:

- Obtained fairly;
- Held for specific purposes and used only for those purposes;
- Relevant, accurate and kept up to date;
- Corrected if shown to be inaccurate;
- Kept no longer than necessary and destroyed when no longer required;
- Protected against loss or disclosure;
- Treated as confidential at all times.

Any breach of this policy could have very serious consequences for an individual or for the Society and will be treated as a serious disciplinary matter.

The letter that is issued to a potential new resident will explain the reason for requiring personal information. This letter will also confirm that the data collected for one purpose will not be used (or passed to other parties) for another purpose.

Information to be kept confidential

All sensitive information will be kept and handled confidentially, whether the information has been received formally, informally or discovered by accident. Broadly, this means

- Anything of a personal nature thatis not a matter of public record about a resident, applicant, staff member trustee, volunteer or society member.
- Sensitive organisational information which could be used to damage the association or threaten the security of property or buildings;
- Tenders and quotations for services and works.

Personal information may be kept in paper or computer file format. It will be stored securely – either in locked cabinets or boxes or on the Society's computer, at our registered office or in the home of our Secretary (or one of our volunteers who may temporarily be providing cover).

Access to sensitive information

Staff, trustees and volunteers will generally have access to all information that they genuinely need to know to carry out their work and have a duty to respect the confidentiality of all personal information held by the Society. It is imperative that confidential information about a resident is not disclosed to another resident, nor should staff and volunteers gossip about residents to one another.

Wherever possible, staff, trustees and volunteers will explain the purpose of recording potentially sensitive personal information and the people likely to have access to it before it is disclosed, so that informed consent can be obtained. If this causes concern, special arrangements for recording and access will be made.
Residents in shared housing are likely to be aware of personal information about other residents and are expected to respect their right to privacy.
It is particularly important to keep secure matters referred to in minutes of meetings which may directly or indirectly make reference to individual residents or confidential plans or actions of the society.

Privacy
The Resident Handbook issued to new residents will confirm that their room is private and personal to them; that they will have their own key; that they may invite visitors into their room; no one will enter their room without permission except in an emergency.

Appendix:
Self Assessment of GDPR requirements
(based upon the on-line Data Protection Toolkit provided by the Information Commissioners Office).

Items		Not yet implemented or planned	Partially implemented or planned	Successfully implemented	Not Applicable
Step 1: Data protection policy, responsibility and training. Our business					
1.1 Policy	has established an appropriate data protection policy.			*	
1.2 Management responsibility	nominated a data protection lead.			*	
1.3 Training and awareness	provides data protection awareness training for all staff.			*	
Step 2: Registration, privacy notices and subject access. Our business					
2.1 Registration	has registered with the Information Commissioner's Office.			*	
2.2 Privacy notices	has made privacy notices readily available to individuals.			*	
2.3 Responding to subject access requests	has established a process to recognise and respond to individuals' requests to access their personal data.			*	
Step 3: Data quality, accuracy and retention. Our business					
3.1 Data quality and accuracy	has established processes to ensure personal data is of sufficient quality to make decisions about individuals.			*	
3.2 Retention and disposal	has established a process to routinely dispose of personal data that is no longer required in line with agreed timescales.			*	
Step 4: Security. Our business					
4.1 Security	has established an		*		

policy	information security policy supported by appropriate security measures.				
4.2 Outsourcing	ensures an adequate level of protection for any personal data processed by others on your behalf or transferred outside the European Economic Area.			*	

Step 5: Privacy impact assessments. Our business

5.1 Privacy Proofing	has established a process to ensure new projects or initiatives are privacy-proofed at the planning stage.		*		