TITLE	**DATA PROTECTION AND ACCESS TO PERSONAL INFORMATION POLICY**
1 Overview	Abbeyfield Wales Society (AWS) are responsible for the collecting, processing, storing and safe keeping of personal and other information as part of our business activities. We manage personal information in accordance with the Data Protection Act 1998 and aim to comply with the General Data Protection Regulations (GDPR). We are registered as data controllers with the Information Commissioners Office. We take your privacy and the security of that information very seriously. This policy sets out how we meet our obligations under the Data Protection Act to protect the personal information we may hold about you and this policy also sets out your rights to inspect these details. This policy applies to Residents, Staff, Volunteers and Trustees.
2 Data Protection Principles	The Data Protection Act identifies eight data protection principles that AWS is obliged to follow: • Personal data shall be processed fairly and lawfully • Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes • Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. • Personal data shall be accurate and where necessary kept up to date • Personal data processed for any purpose or purposes shall not be kept longer than necessary for that purpose or purposes • Personal data shall be processed in accordance with the rights of data subjects under this Act. • Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and general accidental loss or destruction of, or damage to, personal data. • Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to processing personal data.

3 What Personal data do we collect?	We may collect, process and store information such as: • Tenant/resident names, date of birth, National Insurance number, photographs, contact details and preferences • Tenant/resident demographic data (e.g. ethnicity, religion or belief) • References from landlords, support providers or other people vouching for applicants suitability as a tenant/resident • The details of other family members or people living in our properties or whom provide support or emergency contact for the resident including next of kin • Rent/Fee payments made • Income and expenditure estimates • Repairs requested • Application, referral, support and care forms and plans • Tenancy and or other occupancy agreement or contract • Applications/CV's/references/DBS records/training records for staff, Trustees and volunteers • Physical and mental health conditions • Medications taken/prescribed/needed • Support and care contracts • Support and care plans and details of support and care providers • Complaints about our services • Responses to surveys or involvement initiatives and activities • Allegations of anti-social behaviour • Convictions, proceedings and criminal acts • Correspondence to and from our residents and tenants, their families, or other agencies or advocates acting on their behalf • Recordings of telephone calls made to and from the organisation • CCTV images (where CCTV is provided) and these images will be kept and retained for up to one calendar month to safeguard your health and security. **We may apply markers to your information (for example, in relation to your vulnerability or health status) to enable us to tailor and deliver services to you. It is important that YOU notify us of any changes to YOUR personal information.**
4 How we use your personal information:	We will provide a copy of our privacy notice (See Appendix One), to all residents, potential residents, staff, volunteers and trustees. We will also refer and share links to our privacy notice on our website and emails. **4.1 Tenants and Residents:** We use your personal information for responding to your enquiries,

providing services to you and managing our relationship with you. We will also provide information to:

- Notify you of any changes we are considering or planning to make
- Help us improve our services
- Inform you about our services

We may also anonymise your information, so that it cannot be linked to you, as part of research exercises.

We will always tell you how we will use your information when collecting it from you, for example in an interview, survey form or on our website.

4.2 Job Applicants & Employees:

If you submit a job application or CV to AWS we will use your personal information to process your application and to produce and monitor recruitment statistics. We will not take up references without your prior permission. We will not share or disclose your information unless you have given us your consent or we are required to do so by the law. When you become an employee and where we are required to carry out a Disclosure and Barring Service check we will comply with the law and your rights when carrying out these checks. As an employee we will use you personal data to:

- Ensure we are able to pay you correctly and on time
- To make any deductions required to HMRC or other parties where you have given permission to do so or we are required to do so by an order of the court
- Manage your learning and development
- Maintain supervision records and any disciplinary or grievance records in accordance with our policies in those areas

4.3 Volunteers and Trustees:

As a Volunteer or Trustee you will usually be asked to complete an application form or CV as well as your emergency contact details. We will not take up references without your prior permission. We will not share or disclose your information unless you have given us your consent or we are required to do so by the law. Where we are required to carry out a Disclosure and Barring Service check we will comply with the law and your rights when carrying out these checks.

	We will also collect and maintain records to manage your learning and development.
5 Sharing your personal Information	Access to your information will normally be limited to ourselves (AWS). However, there may be occasions when we disclose your details to others: **5.1 With your consent:** We will usually obtain your consent before referring you to another service, an activity that requires us to share your contact details and background information with the organisation that provides the service. **5.2 Legally Obliged:** We will share specific and relevant information with law enforcement and government agencies or public bodies where we are legally required to do so. Example may include (This list is not exhaustive): • The prevention and detection of crime • The apprehension or prosecution of offenders • The assessment or collection of tax or duty owed to customs and excise • Sharing in connection with legal proceedings • Sharing in relation to physical or mental health of an individual where disclosure is required to protect them or others from serious harm • Research and statistical purposes • Emergency Contact Monitoring centres. We may also share your information with emergency services and local authorities where this is necessary to help them respond to an emergency situation that affects you. **5.3 Contractors and Suppliers:** We may share your personal information with our suppliers and contractors who enable us to provide services to you, or who provide services on our behalf, examples may include specialist call centres as well as maintenance contractors who carry our work in our properties and the contractors who manage our out of hours services and emergency alarm monitoring service. The data shared is the specific

	information the supplier needs to carry out their task, as well as any information that ensures we fulfil our health and safety obligations to the people carrying out that task. Our contractors are also required to ensure that any information we may share with them about you is kept safe and secure and they are required to comply with this policy. AWS remain responsible for the fair and lawful processing of personal data shared with suppliers. We ensure this occurs through setting data protection requirements in contracts that we let with suppliers. **5.4 Utility Companies:** In order to assist utility providers (gas, electricity, Water etc) deliver their services and to collect revenue, we will provide on request names and contact details of new tenants and residents, and forwarding addresses of former tenants, as well as tenancy/occupancy dates. **5.5 Partner Agencies:** We may enter into partnerships with other organisations such as local authorities and the Police. For example, we may join a partnership to help prevent and/or control anti-social behaviour or crime. We will enter into a formal data sharing agreement to govern process and ensure that it is lawful. That agreement will be approved by our Data Protection Manager (CEO) before it is implemented and if needed independent legal advice will be obtained.
6. Working with third party support and care agencies	Resident's personal matters will be discussed within the supported housing and nursing teams and may include a third party support, care agency or a commissioner of services where the individual receives a support or care package from that agency. However, these discussions will be undertaken in confidential meetings. Disclosure of personal information without consent will be exceptional and only if required by law, a court order, or where there is an over-riding health and safety consideration. In our care services we will seek formal permission from you to give authority for us to share that data (See Appendix Two)
8. Protecting Personal	AWS aims to ensure that staff, volunteers and Board members do not

Information	misuse any confidential information, or pass on this information improperly to a third party. We protect personal information by applying technical measures, implementing policies, training for staff, trustees and volunteers and carrying out checks in practice. **8.1 Secure Storage:** Paper files and records containing personal information are kept in secure cabinets. These cabinets are locked when not in use. AWS staff and volunteers are provided with training and guidance before secure handling of records when taken from the office, for example, when carrying out a home visit. We ensure any information on our computer system is secure, accurate, relevant and necessary. All of our computers are secured with passwords, and all staff are trained on our systems. The personal data held on mobile IT devices is minimised and also secured with a password should a device be lost or stolen. **8.2 Telephone Enquiries:** When a tenant or resident or applicant contacts us by phone they will be asked to provide a piece of identifying data (e.g. Date of Birth) to ensure that personal information is only disclosed to the correct person. If a tenant or resident would like someone else to contact AWS on their behalf they need to confirm that to us directly, or if it is an ongoing arrangement complete a Explicit Consent Form (See Appendix Three). **8.3 Online Services:** At the time of adopting this policy AWS has very limited on line services. At present there is no facility within AWS for our service users to access their information on line. **8.4 Complaints:** If someone contacts us to raise a complaint on behalf of a resident we will always seek your permission first before investigating the complaint and responding to the complaint. This is because in responding to the complaint, the person claiming to represent you might view some of your personal data.

	8.5 Rent and/or Fee Enquiries: If you want to make an enquiry about the rent or fees you pay e.g balance of account, payment history etc we will ask you to provide confirmation of your address and date of birth before providing the information. **8.6 Moving out:** If you are a tenant, when you move out of your home we will hold your file for 12 months and then securely destroy the paper files relating to your tenancy, unless we are pursuing you for rent arrears or other debts or we need the information to support any allegation/investigation of anti-social or criminal behaviour. If you are a resident in a nursing home we are currently obliged to retain all records for a period of three years after your occupancy with us has ended. We will then securely destroy the paper files relating to your residency with us. **8.7 Employees, Trustees and Volunteers:** If you are an employee, trustee or volunteer, when you leave we will hold your file for 12 months if you are volunteer or 6 years if you are an employee and then securely destroy the files relating to your employment, trusteeship or voluntary work, unless there is a dispute between us. We will then destroy records once that dispute is resolved.
9 Accessing your personal information	The Data Protection Act 1998 gives you a number of rights in relation to your personal information. You can find out about your rights and obtain further guidance form the website of Information Commissioners Office. https://ico.org.uk/ You have the right to access files or other records containing information relating to: • Your personal tenancy or residency in a nursing homes • Your past tenancies or occupancies • Any proposed tenancies or occupancies

- Care and support plans

Please note the following important information about accessing your personal information:

- You can make your request to any member of staff. All requests are passed by staff to our Data Protection Manager (CEO) to ensure we act in accordance with the Data Protection Act.
- To help us respond, please be specific as you can be about the information you would like to see.
- You will usually be asked to complete a "Subject Access Request" form to access your data (See Appendix Four)
- We will make NO charge for accessing your data but may make a nominal charge if you ask us to photocopy any documents and we will tell you in advance what that charge will be.
- Under the legislation we have One Calendar Month from the date you make a request to see the information to provide it to you.
- You have the right to ask us to delete or change any inaccurate information held on our files. We consider all requests and will change or delete information that we agree is inaccurate.
- You have the right to have personal data erased (or forgotten), this is not a unilateral right, this applies when the information is no longer needed for the purpose for which it was originally collected, or the subject withdraws their consent (where that was the legal basis for processing)

Because we also need to respect the rights of others, we CANNOT make the following information available to you:

- Information relating to, or identifying a third party, unless that person has given their written permission.
- Information from other agencies such as social services, Doctors, Health Boards or lawyers which could reasonably be expected to be treated as confidential
- Information which could cause or lead to physical or mental harm.

The decision to refuse an individual access to personal information about them is taken by the Data Protection Manager (CEO).

If you receive support or care services from us:

	• You can have immediate access to your all part of the file that contain your support or care plans and any reviews of those plans • If you wish to review the full contents of your file, you must put this request in writing and we will aim to provide you with access within 24 hours of receipt of the request where this is feasible. We will identify ourselves and provide a contact number for you to confirm our identity on request when contacting you about our services.
7 Linked Policies	Confidentiality Policy & Procedure Privacy NoticeICT Access Control Policy Information Security Policy Professional Boundaries Policy Records Retention Policy and Schedules
8 Legislation / Regulation	Data Protection Act 1998 GDPR Regulations
9 Review	Adopted by Abbeyfield Wales Society's Board on: 03/09/2018 To be reviewed by Abbeyfield Wales Society's Board on: 03/09/2021