

THE ABBEYFIELD FERRING SOCIETY LTD POLICY & PROCEDURE/GOOD PRACTICE GUIDELINES

Policy Ref:	AF015	Effective date:	March 2019
Owner:	Abbeyfield Ferring Society	Review date:	March 2021

Title:	Data Protection Policy and Procedure
1. Background	<p>Abbeyfield Ferring Society must process personal data in line with the law and guidance provided from time to time by the Information Commissioner's Office.</p> <p>Abbeyfield Ferring Society is registered with the Information Commissioner to process personal data.</p>
2. Objectives	<p>Through the delivery of this policy we aim to:</p> <ul style="list-style-type: none"> • Ensure adequate protection of personal data of our employees, volunteers, residents, service users and donors. • Enable our employees and volunteers to recognise personal data and sensitive personal data to ensure they are processed appropriately. • Clarify the reporting lines in case of data protection breach or risk of such a breach occurring and in general. • Provide practical guidance on what behaviour is expected from employees and volunteers to ensure secure and appropriate processing of personal data.
3. Scope	<p>This policy applies to all Abbeyfield Ferring Society staff, agency staff, volunteers and Executive Committee.</p> <p>Third party companies and individuals who work with Abbeyfield Ferring Society that have access to any personal information held by Abbeyfield Ferring Society must be contractually required to comply with this policy.</p> <p>During the course of Abbeyfield Ferring Society's activities we collect, store and process personal information about people, and we recognise the need to treat it in an appropriate and lawful manner.</p> <p>The types of information that we may be required to handle include details of current, past and prospective employees, volunteers, suppliers, donors, residents and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how we may use that information.</p> <p>This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.</p>
4. Policy	<p>Introduction</p> <p>This policy sets out Abbeyfield Ferring Society's general rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.</p>

THE ABBEYFIELD FERRING SOCIETY LTD POLICY & PROCEDURE/GOOD PRACTICE GUIDELINES

Policy Ref:	AF015	Effective date:	March 2019
Owner:	Abbeyfield Ferring Society	Review date:	March 2021

	<p>The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy. The Data Protection Compliance Manager is Abbeyfield Ferring Society's Chief Operating Officer. Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Compliance Manager.</p> <p>If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with your line manager or the Data Protection Compliance Manager.</p>
4.1.	<p>Definition of Data Protection Terms</p> <p>Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.</p> <p>Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.</p> <p>Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an expression of opinion about the individual (such as a performance appraisal).</p> <p>Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. The Abbeyfield Ferring Society is the data controller of all personal data used in its business.</p> <p>Data users include employees, including volunteers whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.</p> <p>Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.</p> <p>Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it.</p>

THE ABBEYFIELD FERRING SOCIETY LTD POLICY & PROCEDURE/GOOD PRACTICE GUIDELINES

Policy Ref:	AF015	Effective date:	March 2019
Owner:	Abbeyfield Ferring Society	Review date:	March 2021

	<p>Processing also includes transferring personal data to third parties.</p> <p>Phishing is a method used by fraudsters to access valuable personal details and credentials, such as user names and passwords. It involves sending emails or other electronic communications (instant messaging, texts, etc.) containing malicious attachments or website links in an effort to infect computers or mobile devices, or to convince users to supply sensitive personal information.</p> <p>Sensitive Personal Data This includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Information about a resident's physical or mental health, for example, therefore amounts to sensitive personal data. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.</p>
4.2.	<p>Data Protection Principles Anyone processing personal data must comply with the eight enforceable principles of data protection set out in the Act. These state that personal data must be:</p> <ol style="list-style-type: none"> 1. Processed fairly and lawfully 2. Processed for limited purposes and in an appropriate way 3. Adequate, relevant and not excessive for the purpose 4. Accurate 5. Not kept longer than necessary for the purpose 6. Processed in line with data subjects' rights 7. Secure 8. Not transferred to people or organisations situated in countries without adequate protection
4.3.	<p>Fair and Lawful Processing The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. In addition to the information that the data controller is The Abbeyfield Ferring Society and that its representative is the Data Protection Compliance Manager / Office Manager, the data subjects are entitled to be told why we are collecting their data and what we intend to use it for including to whom the data may be disclosed or transferred.</p> <p>For this reason, any website operated by Abbeyfield Ferring Society must include a Privacy Statement, explaining how users' personal information is collected and used.</p>

THE ABBEYFIELD FERRING SOCIETY LTD POLICY & PROCEDURE/GOOD PRACTICE GUIDELINES

Policy Ref:	AF015	Effective date:	March 2019
Owner:	Abbeyfield Ferring Society	Review date:	March 2021

	<p>For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. For example, Abbeyfield Ferring Society employees consent to Abbeyfield Ferring Society processing their personal data when they sign their employment contract.</p> <p>When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required. For example, if the resident's sensitive data is held by Abbeyfield Ferring Society with the resident's consent in order to arrange the resident's care, Abbeyfield Ferring Society will be entitled to disclose that information on resident's admission to the A&E if withholding the information was likely harm the resident's vital interests.</p>
4.4.	<p>Processing for Limited Purposes</p> <p>Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs. For example if Abbeyfield Ferring Society hold personal data of a volunteer for the health and safety purposes it will not be entitled to direct its marketing emails to the volunteer without first obtaining his or her consent.</p>
4.5.	<p>Adequate, Relevant and Non-Excessive Processing</p> <p>Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.</p>
4.6.	<p>Accurate Data</p> <p>Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.</p>
4.7.	<p>Timely Processing</p> <p>Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data should be kept before being destroyed, please</p>

THE ABBEYFIELD FERRING SOCIETY LTD POLICY & PROCEDURE/GOOD PRACTICE GUIDELINES

Policy Ref:	AF015	Effective date:	March 2019
Owner:	Abbeyfield Ferring Society	Review date:	March 2021

	refer to the Records Retention Policy and Schedules or contact the Data Protection Compliance Manager.
4.8.	<p>Processing in Line with Data Subject's Rights</p> <p>Data must be processed in line with data subject's rights. Data subjects have a right to:</p> <ul style="list-style-type: none"> • Request access to any data held about them by a data controller • Prevent the processing of their data for direct-marketing purposes • Ask to have inaccurate data amended • Prevent processing that is likely to cause damage or distress to themselves or anyone else
4.9.	<p>Data Security</p> <p>Appropriate security measures must be taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.</p> <p>Abbeyfield Ferring Society has in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he puts in place equivalent or otherwise adequate measures himself.</p> <p>Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:</p> <ul style="list-style-type: none"> • Confidentiality means that only people who are authorised to use the data can access it • Integrity means that personal data should be accurate and suitable for the purpose for which it is processed • Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the central computer system instead of individual PCs <p>Security procedures include:</p> <ul style="list-style-type: none"> • Entry controls: These should be installed in all areas where data is processed. Any stranger seen in entry-controlled areas should be reported • Secure lockable desks and cupboards: Desks and cupboards should be kept locked if they hold personal data or confidential information of any kind (personal information is always considered confidential). • Methods of Disposal: Paper documents should be shredded. CD-ROMS and Memory Sticks should be physically destroyed when they are no longer required • Equipment: Data users should ensure that individual monitors do not show

THE ABBEYFIELD FERRING SOCIETY LTD POLICY & PROCEDURE/GOOD PRACTICE GUIDELINES

Policy Ref:	AF015	Effective date:	March 2019
Owner:	Abbeyfield Ferring Society	Review date:	March 2021

	<p>confidential information to passers-by and that they log off from their PC whenever it is left unattended.</p> <p>For further guidance on IT security measures which should be taken, please refer to the following Abbeyfield Ferring Society policies:</p> <ul style="list-style-type: none"> • Computer and Internet Usage Policy • ICT Access Control Policy • Phishing Guidance Advisory
4.10.	<p>Dealing with Subject Access Requests</p> <p>A formal request from a data subject (or their authorised representative) for information that we hold about them must be made in writing. Any member of staff who receives a written request should forward it to the Data Protection Compliance Manager immediately. Subject access requests will be dealt with in accordance with the guidance contained in the Access to Personal Records Policy.</p>
4.11.	<p>Providing Information to Third Parties</p> <p>Any member of staff dealing with enquires from third parties should be careful about disclosing any personal information held by us. In particular they should:</p> <ul style="list-style-type: none"> • Check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested • Suggest that the third party put their request in writing if there are any doubts about their identity or entitlement to the information requested. This can then be checked • Refer to the line manager or the Data Protection Compliance Manager for assistance in difficult situations. No-one should be bullied into disclosing personal information • When providing information to a third party, do so in accordance with the eight protection principles (see above)
4.12.	
5. Training and Guidance	<p>All employees and volunteers are required to complete data protection and information security training when they join Abbeyfield Ferring Society at their induction, with annual refreshers thereafter. Staff that lead on data protection matters will receive more comprehensive training.</p> <p>Data Protection Compliance Manager is responsible for organising training and can also provide additional training for employees or teams who would benefit from this. Please contact them if you would like to arrange this.</p>
6. Supporting Appendices	N/A
7. Linked policies	<ul style="list-style-type: none"> • Access to Personal Records Policy

THE ABBEYFIELD FERRING SOCIETY LTD POLICY & PROCEDURE/GOOD PRACTICE GUIDELINES

Policy Ref:	AF015	Effective date:	March 2019
Owner:	Abbeyfield Ferring Society	Review date:	March 2021

	<ul style="list-style-type: none"> • Computer and Internet Usage Policy • Confidentiality Policy & Procedure • CCTV Policy & Procedure • ICT Access Control Policy • Information Security Policy • Professional Boundaries Policy • Records Retention Policy and Schedules • Phishing Guidance Advisory
8. Legislation / Regulation	Data protection Act 1998
9. Review	Every 2 years, subject to any regulatory or legislative updates.
10. Procedure / Guidance	N/A