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

Policy Ref:	AF037	Effective date:	August 2017
Owner:	Abbeyfield Ferring Society	Review date:	August 2018

Title:	**INFORMATION SECURITY POLICY**
1. Background	Information security risks must be managed efficiently, collectively and proportionately, to achieve a secure confident working environment and ensure we are complying with best practice and legal and regulatory requirements. This is key in enabling Abbeyfield Ferring Society to meet its operational and strategic objectives.
2. Objectives	Information security risks must be managed efficiently, collectively and proportionately, to achieve a secure confident working environment and ensure we are complying with best practice and legal and regulatory requirements. This is key in enabling Abbeyfield Ferring Society to meet its operational and strategic objectives.
3. Scope	This policy applies to all established staff, Trustees, agency staff and volunteers. Third party companies and individuals who work with Abbeyfield Ferring Society and have access to any of the Society's information assets must be contractually required to comply with this policy.
4. Policy 4.1	**Definitions** In this policy, "information security" is defined as: ***"preserving":*** this means that management, all full time or part time staff, volunteers, subcontractors, project consultants and any external parties are made aware of their responsibilities (which are defined in their job descriptions or contracts) to preserve information security and report any potential or actual security breaches. All staff will receive information security awareness training and more specialised staff will receive appropriately specialised information security training. ***"confidentiality":*** This involves ensuring that information is only accessible to those authorised to access it and therefore to prevent both deliberate and accidental unauthorised access to Abbeyfield's information and proprietary knowledge and its systems including its network(s) and website(s). Access will be granted in line with job role using the principle of 'least possible privileges'. ***"integrity":*** This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency including for networks, web sites and data back-up plans, and security incident reporting. Abbeyfield Ferring Society must comply with all relevant data-related legislation in those jurisdictions within which it operates. ***"availability":*** This means that information and associated assets should be accessible to authorised users when required and therefore logically & physically secure. The

Policy Ref:	AF037	Effective date:	August 2017
Owner:	Abbeyfield Ferring Society	Review date:	August 2018

	computer network(s) must be resilient and Abbeyfield Ferring Society must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans in place and tested. ***"of the physical (assets)":*** The physical assets of Abbeyfield Ferring Society including but not limited to computer hardware and mobile devices, network hardware and data cabling, telephone systems, filing systems and physical data files. ***"and information assets":*** The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, web sites, PCs, laptops, mobile phones and PDAs as well as on CDs, USB sticks, backup tapes and any other digital or analogue media, and information transmitted electronically by any means. In this context "data" also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc). ***"throughout Abbeyfield":*** Abbeyfield and such members and partners that are part of the organisation's integrated network, have signed up to our security policy and have accepted all associated policies and procedures. ***"security incident":*** any incident or activity that causes or may cause a breakdown in the availability, confidentiality or integrity of the physical or electronic information assets of Abbeyfield. **"phishing":** 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.
4.2	**Introduction** The management of Abbeyfield Ferring Society are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout Abbeyfield Ferring in order to protect the privacy of its residents and service users, to preserve its reputation and satisfy its legal and contractual obligations. This is achieved by: • Treating information security as a critical business issue. • Supporting the implementation, operation and maintenance of an operational security framework. • Creating a security-aware work environment.

Policy Ref:	AF037	Effective date:	August 2017
Owner:	Abbeyfield Ferring Society	Review date:	August 2018

	• Implementing controls that are proportionate to risk. • Achieving individual accountability for compliance with information security policies and supporting procedures.
4.3	**Roles and Responsibilities** The Chief Operating Officer will be responsible for providing help and guidance on all matters relating to information security. All individual users are responsible for ensuring that no breaches of the policy result from their actions and for reporting any breach or suspected breach of it.
4.4	**Security Incident Management** It is the responsibility of all users to report any incident, threats, weakness or vulnerabilities as soon as they are detected. The management of any security incident will need to take account of the severity of the issue and how urgently it should be dealt with. Guidance is provided below but if in doubt, you should contact the Information Security Officer or Legal Team for assistance. **Minor Incident** • Passwords • Anti-malware issues/virus outbreaks • Phishing attempts • Missing files • Minor equipment theft or loss Any minor incidents concerning IT security within Abbeyfield Ferring Society should initially be raised with the COO. All incidents will be reviewed on a regular basis. **Major Incident** • Risk to Abbeyfield's reputation • Loss of Financial or Medical information • Loss of any other confidential or personal (including sensitive personal) data • Data Protection breach • Larger scale equipment theft or loss • Known unauthorised access • Breach of confidentiality issues

Policy Ref:	AF037	Effective date:	August 2017
Owner:	Abbeyfield Ferring Society	Review date:	August 2018

	The COO and the Chairman of the Board must be notified as soon as possible of all major incidents and will provide further guidance as necessary. Any actual or potential data protection breaches must also be reported to the COO. It is likely that other Managers will be involved in managing the investigation of most incidents. Individuals reporting incidents should therefore also notify their line manager where appropriate. The Executive Committee will be provided with regular reports of all major incidents by the COO. If there are a large number of incidents, then it may be necessary to discuss the issues and make recommendations for policy change, if relevant. Any breaches of this policy or any of its supporting policies and standards will be taken seriously and may result in disciplinary action.
5. Finance	TBC
6. Supporting Appendices	
7. Linked policies	• Confidentiality Policy & Procedure • Data Protection Policy • Mobile Devices Security Policy
8. Legislation / Regulation	Data Protection Act 1998
9. Review	Every year, subject to any regulatory or legislative updates.
10. Procedure / Guidance	