Information Security

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 The Dales Ltd (ATD) to meet its operational and strategic objectives.

2. Objectives

Through the delivery of this policy we aim to:

- Enable ATD to maintain the confidentiality, integrity and availability of its information assets and systems.
- Respond to and remedy security incidents in a timely and effective manner; and
- Provide practical guidance on avoiding inadvertent data disclosure (Phishing).
- Comply with all relevant and current legislation.

3. Scope

This policy applies to all established staff, agency staff; volunteers; and staff based at the head office at Grove House.

Third party companies and individuals who work with ATD and have access to any of ATD'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:

4.1.1. 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.

4.1.2. 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 ATD's information and proprietary knowledge, and its

systems including its network(s) and website(s). Access will be granted in line with job roles using the principle of 'least possible privileges'.

4.1.3. 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 included for networks, web sites and data back-up plans, and security incident reporting. ATD must comply with all relevant data-related legislation in those jurisdictions within which it operates.

4.1.4. Availability

This means that information and associated assets should be accessible to authorised users when required and therefore logically & physically secure. The computer network(s) must be resilient and ATD 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.

4.1.5. Physical Assets

The physical assets of ATD including but not limited to computer hardware and mobile devices, network hardware and data cabling, telephone systems, filing systems and physical data files.

4.1.6. 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).

4.1.7. Throughout ATD

ATD 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.

4.1.8. 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 ATD.

4.1.9. Phishing

A method used by fraudsters to access valuable personal details and credentials, such as usernames and passwords. It involves sending emails or other electronic communications (instant messaging, texts, etc.) containing

malicious attachments or website links to infect computers or mobile devices, or to convince users to supply sensitive personal information.

4.2. Introduction

The Senior Leadership Team (SLT) of ATD are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout ATD 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.
- Implementing controls that are proportionate to risk; and
- Achieving individual accountability for compliance with information security policies and supporting procedures.

4.3. Roles & Responsibilities

4.3.1. Business Support Manager (BSM)

The Data Protection Officer within ATD is the BSM and will be responsible for ensuring adherence to the principles of the Data Protection Act, creating/maintaining the information security framework and providing help and guidance on all matters relating to information security.

4.3.2. Employees

Individual users are responsible for ensuring that no breaches of the policy framework 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 BSM for assistance.

4.4.1. Minor Incident

- Passwords.
- Anti-malware issues/virus outbreaks.
- Phishing attempts.
- Missing files; and/or
- Minor equipment theft or loss.

Any minor incidents concerning IT security within ATD should initially be raised with the BSM. ATD's IT Consultant will be able to log and deal with these incidents or pass the incident to the BSM to investigate further. All incidents will be reviewed on a regular basis.

4.4.2. 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; and/or
- Breach of confidentiality issues.

The BSM 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 BSM.

It is likely that other Managers will be involved in managing the investigation.

4.5. Breaches of this Policy

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, Value for Money & Social Value

N/A

6. Supported Appendices

N/A

7. Linked Policies

Access to Personal Records (LG039P)
CCTV (LG005P)
Computer and Internet Usage (LG009P)
Confidentiality, Privacy & Dignity (R005P)
Data Protection (LG031P)
ICT Access Control (LG022P)
Records Retention (LG015P)
Use of Artificial Intelligence (AI) (LG046P)

8. Legislation/Regulation

Data Protection Act 1998 (DPA)
UK General Data Protection Regulation 2018 (UK GDPR)

9. Review

Every 2 years, subject to any regulatory or legislative updates.

10. Procedure/Guidance

N/A