Computers, Mobile Devices & Internet Usage

1. Background

All individuals using Abbeyfield The Dales Ltd. (ATD) IT network shall adhere to strict guidelines concerning appropriate use of ATD's computers/mobile devices and network resources.

2. Objectives

Through the delivery of this policy we aim to:

- Delineate policies and procedure for accessing ATD's IT network and/or accessing the Internet through ATD's IT network to ensure the security and integrity of ATD's information and compliance with relevant legislation.

3. Scope

This policy covers all individuals working for ATD at all levels and grades, including senior managers, officers, directors, employees, volunteers, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff (collectively referred to as staff in this policy).

This policy applies to all staff with access to the Internet and related services through ATD's network infrastructure. Internet related services include all services provided with the TCP/IP protocol, including but not limited to Electronic Mail (e-mail), File Transfer Protocol (FTP) and World Wide Web (WWW) access.

4. Policy

4.1. Definitions

4.1.1. Internet

The international computer network of networks that connect business institutions, academic, government, private users etc.

4.1.2. Intranet

A private network contained within an organisation, using web technology to share information internally.

4.1.3. Phishing

A method used by fraudsters to access valuable personal 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. Acceptable Use – Computers/Mobile Phones and Internet

- ATD's resources are provided on the understanding that they are to be used for business purposes and used in a common-sense way that satisfies ATD's policy, although it is

anticipated that occasional use of ATD's resources for personal reasons may be necessary.
- Internet use for personal reasons is limited to appropriate breaks.

4.3. Inappropriate Use – Computers/Mobile Devices and Internet

- Internet access shall not be for any illegal or unlawful purpose. Examples of this are the transmission or download of violent, threatening, defrauding, pornographic, obscene, or otherwise illegal or unlawful materials.
- Use of ATD e-mail service shall not be made to harass, intimidate or otherwise annoy another person.
- ATD's internet and e-mail connections shall not be used for political purposes or to conduct personal business.
- Staff shall not use ATD network for personal gain such as selling ATD's user access login ID's. Internet access through the ATD network shall not be for or by performing unauthorised work for profit.
- Staff shall not attempt to circumvent or subvert security measures on ATD's network resources, or any other system connected to or accessible through the internet.
- Staff shall not make or use illegal copies of copyrighted material, store such material on ATD equipment, or transmit such material over the ATD network.
- Staff shall not download any software from the Internet; this includes screensavers, music, games etc.
- Staff shall not download any personal material on ATD resources.
- No software other than software supplied by the IT department shall be loaded onto ATD equipment.
- Chat room software may not be used on the ATD network with the exception of Microsoft Teams, Zoom and any other secure channels for business purposes.
- Staff shall not download or stream copyrighted material such as MP3 files, film and video files, without appropriate approval.
- Staff shall not connect any device to the ATD network or IT systems which has not been authorised by ATD; and
- Staff shall not store ATD data on any non-authorised equipment.

4.4. E-Mail Etiquette

- Staff shall ensure all communication through e-mail is conducted in a professional manner. All e-mails should be courteous. The use of suggestive, vulgar, or obscene language is prohibited.
- Users should be mindful of the tone of their communications and should take responsibility to consider the impact of their email upon the reader.
- ATD users must not send unprotected sensitive or confidential information (such as care records) externally. Such information should be securely encrypted and only sent where all necessary permissions have been obtained.
- ATD users shall not reveal private or personal information through ATD e-mail without clear and specific written approval from management.
- Users should ensure that e-mail messages are sent to only those users with a specific need to know. The transmission of e-mails to large groups, use of e-mail distribution lists, or sending messages with large file attachments should be avoided. Internal emails should provide relevant documents by means of a hyperlink rather than as attachments wherever possible.
- Use of 'CC' should be limited to third parties with a need to know the information being transmitted. It is generally not expected that a person cc'd would reply to an email. Careful consideration should be given before cc-ing a person into an email as the motive for such an action may not be clear.

- Large scale communications, i.e. the same message to many people internally or externally; should be avoided. However, where circumstances require this, all recipients should be bcc'd to protect the individual's identity and/or to avoid a recipient replying to all and potentially disclosing information not relevant to the other recipients.
- E-mail privacy cannot be guaranteed. For security reasons, messages transmitted through ATD's e-mail system or network infrastructure are the property of ATD and are, therefore, subject to inspection.
- Users shall ensure that the standard e-mail signature has been added and that it is applied to both new and reply messages.
- For planned absences, the out of office assistant should be used, and it should indicate the duration of the absence and who else could be contacted if a matter is urgent. It should be turned off as soon as it is no longer relevant; and
- Personal emails should not be sent via a business email, staff should be mindful that all communications can be monitored, and staff will be held accountable for improper use.

4.5. Computer/Mobile Devices and Internet Usage – Security

- Users who identify or perceive an actual or suspect security problem shall immediately contact the Business Support Manager.
- Network users shall not reveal their account passwords to others, or to allow any other person, employee or not, to use their accounts. Similarly, users shall not use other staff's accounts.
- All use of IT assets is subject to the Financial Controller's consent; and
- Phishing – Be suspicious of any email or communication with urgent requests for personal information, or emails with questionable attachments.

4.6. Computer/Mobile Devices and Internet Usage – Penalties

- Breaches of this policy will be investigated and may, for employees, result in disciplinary action up to and including dismissal; and
- For contractors, this may provide a reason for the termination of the contract under which their services are provided to ATD.

5. Finance, Value for Money & Social Value

N/A

6. Supported Appendices

N/A

7. Linked Policies

ICT Access Control (LG022P)
Confidentiality, Privacy & Dignity (R005P)
Data Protection (LG013P)
Access to Personal Records (LG039P)
Information Security (LG023P)
Use of Artificial Intelligence (AI) (LG046P)

8. Legislation/Regulation

Data Protection Act 1998
Computer Misuse Act 1990
Copyright, Designs and Patents Act 1988
Malicious Communications Act 1988
Digital Economy Act 2010

9. Review

Every 3 years, subject to any regulatory or legislative updates.

10. Procedure/Guidance

N/A