Section: Technology

Computer Use Policy	Date Approved:	November 2022
	Director Responsible:	Vice President, Finance and Organizational Services
	Date for Review:	November 2023

PURPOSE

To set forth appropriate guidelines and responsibilities for the use of KidsAbility computing resources including individual PCs (servers, desktops, laptops), software (all end-user applications and operating systems) and all hardware (printers, digital devices, etc.). Anyone wishing to use a personal device to support their work must have it encrypted and administered by the IT department and responsible conduct is expected as outlined below.

All new employees and volunteers are required to review this Computer Use Policy and sign the Computer Use Acknowledgement form as a condition of employment or engagement.

DEFINITIONS

SCOPE

The entire organization

POLICY

It is the policy of KidsAbility to utilize technology as a means to enable staff to help achieve the mission of the organization and to work effectively in partnership with other service providers.

KidsAbility "computing resources" refers to the computer hardware, software, data, and network resources owned and/or administered by KidsAbility. All information on KidsAbility-owned and/or administered computers and networks is the property of KidsAbility. Some computers may be considered 'bookable' devices, reserved in advance and used by a variety of staff.

All access to the KidsAbility network computer and systems available to staff and volunteers is "password protected" as a best practice for system security and data integrity.

Appropriate Use Statement

KidsAbility staff, contractors and volunteers are required to use computer resources as part of their job function.

It is the responsibility of all who use these resources to respect the intellectual, access and privacy rights of others who use them.

User Responsibilities

The responsibilities accompanying the use of KidsAbility computer resources are as follows:

1. Users are responsible for the integrity of their login and passwords, their own data files (e.g., reports) and email.
2. All users are expected to comply with the KidsAbility policies that protect the privacy of information of clients and co-workers.

3. All users are expected to report any issues, violations, viruses or malfunctions in a timely and reasonable manner.
4. All users are expected to be good custodians of the resources and regularly delete unnecessary files from shared computing resources (server drives), including e-mail.

Confidentiality and Privacy

- KidsAbility is governed by the Personal Health Information Protection Act (PHIPA). All staff, contractors and volunteers are required to sign a confidentiality agreement as a term of employment/engagement.
- If a person chooses to work on documents with personal health information or access this work from outside of the KidsAbility network then the document is to be transferred (copied) to a secure removable device (e.g. an encrypted memory stick). These are available through the IT staff. Alternatively, supervisors may approve secure remote access for staff as per the Remote Access policy.
- KidsAbility staff are absolutely not permitted to forward, copy or attach client reports to, or within, an unsecured email (e.g. MS Outlook). If a parent/client insists on receiving a report via email the following steps ***must be followed***:
    1. The parent must make a request by email stating:
        - which report they want emailed; and that
        - they acknowledge KidsAbility is not responsible for security of the report once it leaves KidsAbility's domain
    2. The CSA documents the request in a CONSENT NOTE in Goldcare and attaches the email directive.
    3. CSA may only send an encrypted PDF report protected by password to the family using the email sent to KidsAbility using no identifying information in the subject line. If the family provides the email address verbally or on a form, the CSA must first email the family to ensure it has been input correctly.
    4. The password to open the document should be sent with a 6 hour delay so that if the email is sent to the wrong address, there is sufficient time to recall the password email to keep the original document secure. Please refer to IT's "How To" document for further instructions.

- Third party 'cloud services' services (e.g. 'drop box' or google docs) are not encrypted and therefore do not meet privacy standards for personal health information therefore should NOT be used.

Software Licensing, Installation and Use

- ONLY authorized software is permitted on a KidsAbility computer. The IT staff are not permitted to install or support personal-use applications.
- The IT department must be involved in the purchase of all other software that is required by employees. This also applies to software used solely for therapy purposes on stand-alone therapy computers (e.g. ACS, iPad). All purchased software licenses and media are the property of KidsAbility.
- KidsAbility has a strategy for tablet applications which may include music. Any other Music and video file downloads on to KidsAbility computers is not allowed (e.g. for iPods, Zune, MP3).
- Reproduction of copyrighted or licensed software is illegal and is not condoned by the KidsAbility. No computer software of any kind is to be installed or downloaded on Centre computers.
- Office computers are not to be used for storing personal files, data, games or photos.

Hardware Installation & Maintenance

- Installation and Maintenance of computer hardware is the sole responsibility of the I.T. department. Contact helpdesk@kidsability.ca for assistance.
- No employee should open any computer attempting to repair a problem; this could void any vendor warranty on the hardware.

Damage / Viruses

- Employees will not willfully destroy, alter, damage or steal computer resources (hardware, software or data) belonging to the KidsAbility or to other users.

- Malware (viruses, trojans, and other destructive computer programs) represent a serious threat to the operation of the Centre and to the Centre's data. All employees are expected to take reasonable precautions to protect against introducing viruses or malware and immediately informing the I.T. Helpdesk should a virus be discovered.

Attached Portable/Personal Devices (e.g. the iPod/iPhone devices)

- Connecting personal portable devices (e.g. the iPod/iPhone devices, external hard drive or USB) to your KidsAbility computer systems is forbidden; portable devices have the ability to transfer information, possibly against policy, in a manner that exposes the asset to great risk.
- Any personally identifiable information stored on MP3 players that ends up on your desktops via iTunes has *Data Protection Act* implications for KidsAbility.
- The software supporting downloadable music and videos (e.g. ITunes) requires a license and use of this software on a KidsAbility machine is illegal. (*Footnote: If music is required and will not interrupt daily work activities, the use of an iPod/Zune/Creative/MP3 player with ear phones is acceptable.)*

E-Mail Usage

KidsAbility deploys email as a critical communication strategy and all employees are provided with an email account. Employees are expected to conduct themselves ethically and professionally when using e-mail utilizing civil standards of communication and respectful of the rights of others at all times. Chain mail is deemed inappropriate in the workplace and not to be shared.

- Staff is expected to use the e-mail account and address allocated to them by the IT department. The set-up and use of Hotmail, Gmail or any other free Web e-mail account is not permitted.
- Refer to ***Confidentiality and Privacy*** section (below) when using email for client related communications.
- ONLY at the discretion of the supervisor will an employee's personal smart phone be configured to receive KidsAbility email with a signed agreement that the device will be remotely wiped clean if lost, stolen, or the employee leaves their employment at KidsAbility. Lost or stolen devices represent a confidentiality breach due to KidsAbility email content and contacts; non-KidsAbility devices cannot be remotely wiped clean if lost or stolen.

Internet Access & Use

- Staff are expected to use good judgment and discretion when using the internet. Use of the Internet for browsing for personal purposes (e.g. surfing, planning vacations) is to be done on personal time and to be done responsibly.
- Downloading, copying, viewing, or distributing hate literature, pornographic or offensive material on the Internet from or through the services KidsAbility provides is strictly prohibited. Accessing gambling sites of any sort is prohibited. These activities violate KidsAbility policies and procedures and may be subject to criminal prosecution. Unauthorized employee involvement in these activities will result in internal disciplinary action and can include termination. Should you require access to Internet sites which may be sensitive in nature for the sole purpose of clinical activities you must obtain supervisor's approval.

Mobile Computing

Refer to Admin policy Mobile Computing and Equipment Lending Policy

SYSTEM ACCOUNTS

USE OF ACCOUNTS

- The HelpDesk, upon approval from the respective supervisor or manager, will assign all KidsAbility employee accounts.
- The System Administrator(s) of the Client Information System (e.g. GoldCare) will request a new login and password for therapy staff from the system vendor (e.g. Campana Systems Inc.). The System Administrator(s) will assign the security access and permissions for that individual within the system.

- Employees assigned a computer account at KidsAbility will be responsible for the legitimate use of their account and must take precautionary action to reduce the possibility of illegal use by unauthorized persons. **Therefore, employees must not allow others to utilize their personal accounts. As a precaution do not leave yourself logged into the network unattended where others may gain access to your account. Your workstation must be *locked* whenever you are not in front of it**
- No employee will employ the KidsAbility network to attempt to gain unauthorized access to ANY computer system either within our network or on the Internet.
- Employees will not invade the security of personal and Centre accounts. Attempts to decipher passwords discover unprotected files, or to decode encrypted files are not allowed and these actions will be subject to discipline.

PASSWORD PROTECTION

- All employees using the system will assign their own personal password and change their password(s) to ensure security whenever prompted to do so by the computer or the IT Department.
- **Do not give out or share your personal passwords with other individuals.**
- Network passwords protocols:
    - should be 6-10 characters in length
    - Does not contain your user name, real name, or company name
    - Does not contain a complete dictionary word
    - Is significantly different from previous passwords. Note: passwords that increment (password1, password2, password3 …) are not strong
    - The Client Information System (e.g. GoldCare) has similar password protocols; refer to the user manual or consult your System Administrator for specifics
    - Forced change every 6 months, but highly recommend that it be changed frequently

Group	Example
Lowercase letters	a, b, c, ...
Uppercase letters	A, B, C, ...
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Non-alphanumeric (symbols)	( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? /

Enforcement of Policies

Authority for KidsAbility computing resources rests with the Vice President, Finance and Operations who is responsible for Technology. Upon learning of an alleged violation the Director will make a determination with the Leadership team to access the individual's files and email so an appropriate investigation can be undertaken. Any activity with the potential to violate criminal legislation will be referred to the appropriate officials.

Upon termination of employment your network and system access is terminated to all files and emails. The supervisor or other staff may be granted access to the files and emails in order to conduct the business of the organization.

Computer Use Policy Acceptance FORM

All employees and volunteers are expected to read and accept this Computer Use Policy as a condition of employment or engagement with KidsAbility. The Acceptance form is found in the Forms Drawer.

REFERENCES

S:\FORMS DRAWER\ADMIN\Technology forms
S:\Publications\Information Technology\HOW TO

Mobile Computing and Equipment Lending Policy Remote Access to KidsAbility Network

Electronic Communication to Share Personal Health Information Policy

APPENDICES