Computer and Technology Resource Usage Agreement

The BC Centre for Ability Association (the Centre) provides a variety of electronic communications systems for use in carrying out its business. All communication and information transmitted by, received from or stored in these systems are the property of the Centre and, as such, are intended to be used for job-related purposes only. Users are required to sign the Computer and Technology Resource Usage Agreement before receiving access to the various systems in use at the Centre.

The following policies regarding access to and disclosure of data on any CENTRE's electronic communication system will guide users on using these systems, to ensure personal and the Centre's privacy and security concerns. Users should contact the Information Technology (IT) Department for more detailed information regarding these policies as required.

Monitoring: The Centre provides the network, personal computers, electronic mail and other communications devices for use on Centre business. The CENTRE may access and disclose all data or messages stored on its systems or sent over its electronic mail system. The Centre reserves the right to monitor communication and data at any time, with or without notice, to ensure that Centre property is being used only for Centre business. The Centre also reserves the right to disclose the contents of messages for any purpose at its sole discretion. No monitoring or disclosure will occur without the direction of executive leadership, unless otherwise noted.

Retrieval: Notwithstanding the Centre's right to retrieve and read any e-mail messages, such messages should be treated as confidential by other users and accessed only by the intended recipient. Users are not authorized to retrieve or read any e-mail messages that are not sent to them and cannot use a password, access file, or retrieve and stored information unless authorized to do so.

Passwords: Initial passwords are assigned by the IT Department and should not be given to other uses or persons outside the organization. Users should change the provided passwords as soon as possible using the instructions provided by the IT staff. The Centre reserves the right to override any user selected passwords and/or codes. Users are required to provide the Centre with any such codes or passwords to facilitate access as needed. Periodically, users may be required to change their passwords. At no time should any users allow a temporary, contractor or another user the use of their login. In the case where a user does provide another person access to his/her account, he/she will be responsible for the actions of the individual using his/her account. Passwords should not be stored in computer data files, on the network, or be displayed openly at any workstation.

Initials: _____

Message Content: The e-mail system is not to be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations. The system is not to be used to create any offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability. The Centre's Policy and Procedures Manual or code of conduct shall be considered the prevailing authority in the event of possible misconduct.

Users should note that any data and information on the system will not be deemed personal or private. In addition, the e-mail system may not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

Legal Proceedings: Information sent by users via the electronic mail system may be used in legal proceedings. Electronic mail messages are considered written communications and are potentially the subject of subpoena in litigation. The Centre may inspect the contents of electronic mail messages in the course of an investigation, will respond to the legal process and will fulfill any legal obligations to third parties.

Physical Security: Access to computer rooms will be limited to users who require access for the normal performance of their jobs. Computers with sensitive information installed on the local disk drive should be secured in a locked room or office during non-business hours. The user must seek permission from the relevant Director and inform the IT Department in advance if IT equipment is to be removed from the Centre's property. All equipment removal from the premises by an individual must be documented, including the makes, manufacturers and serial numbers on an IT Department supplied form, and a copy of this form shall be filed in the IT Department folder. If the user leaves the Centre, he or she must return the equipment to the Centre prior to the last day of departure.

Network Security: IT Department will monitor network security on a regular basis. Adequate information concerning network traffic and activity will be logged to ensure that breaches in network security can be detected. IT Department will also implement and maintain procedures to provide adequate protection from intrusion into the Centre's computer systems from external sources. No computer that is connected to the network can have stored, on its disk(s) or in its memory, information that would permit access to other parts of the network. Users should not store confidential personal or business information such as, membership account or credit card account, or passwords within word processing or other data documents (such as Word and Excel).

Initials: _____

Personal Computer Security: Only legally licensed software will be installed on the Centre's computers. Users are expected to read, understand, and conform to the license requirements of any software product(s) they use or install. Software cannot be copied or installed without the permission or involvement of the IT Department. IT Department will configure all workstations with virus protection software, which should not be removed or disabled. Each user is responsible for protecting his/her computer against virus attack by following IT Department guidelines for scanning all incoming communications and media, and by not disabling the anti-virus application installed on his/her workstation. All data disks and files entering or leaving the Centre should be scanned for viruses. All users will log out of the network and restart their computers before leaving the office at night. Users should log off of the network when they will be away from their desk for an extended period.

Backup Procedures: All network resources are backed up nightly, and tapes are rotated on a two-week schedule and stored off site. Nightly backups are stored for two weeks, and a weekly tape will be stored for no more than five weeks. Data stored on the local PC drives is not backed up, and as a result, important data and applications should not be stored on the C: drives of these machines. Users working on especially crucial information are encouraged to backup these projects to the File Server. Users will be responsible for ensuring that no Centre's data is stored on local machines.

Access to the Centre Computers: The Centre will provide computer user accounts to all Centre staff. External people who are determined to be strategically important to the Centre, such as temporary staff, volunteers, or contractors, will also be provided accounts as appropriated, on a case-by-case basis. The supervisor managing these temporary staff/contractors/students/volunteers assumes responsibility for the identification of access requirements and use of the account. Accounts will be revoked on request of the user or supervisor or when the user is no longer involved with the Centre.

Internet Usage: The Internet is to be used for Centre business only. Users with Internet access are expressly prohibited from accessing, viewing, downloading, or printing pornographic or other sexually explicit materials. In addition, users should be mindful that there is no assurance that e-mail texts and attachments sent within the Centre and on the Internet will not be seen, accessed, or intercepted by unauthorized parties.

Software Usage: Users are expected to use the standard software provided by IT Department, or identify applications they need in the course of their work. Users are not permitted to download applications, demos, or upgrades without the involvement of the IT Department. Users will use the standard e-mail system provided by the Centre for official e-mail communications and should not install their own e-mail systems. Additionally, use of instant messaging programs, such as ICQ, AOL Instant Messenger, Microsoft Messenger, EBay, Facebook, Streaming Video/Audio, etc., is prohibited unless otherwise approved by management or the IT Department.

Initials: _____

Failure to comply with all components of the Computer and Technology Resource Usage Agreement may result in disciplinary action up to and including termination of employment/placement at the Centre. Any users who does not understand any part of this Agreement is responsible for obtaining clarification from the Program/Department Supervisor or the IT Department.

I have read and will comply with this Agreement.

_____	_____
User Name (print)	User Signature
_____	_____
Witness Name (print)	Witness Signature
_____	
Date	