Technology

POLICY

Cascadia Society will effectively use technology throughout all of our homes, programs and administrative offices to increase our efficiency. Technology includes but is not limited to: cell phones, walkie-talkies, printers, fax machines, computers, lap-tops, etc. Cascadia recognizes the value and confidentiality of its electronic data and as such ensures all electronic resources i.e. computers are protected and updated with anti-virus and security protection.

Confidential electronic records of companions and coworkers are backed up on the network and stored off-site in a secure setting. Documentation produced or stored electronically meets applicable legislation and society policies. Files and records are held secure and confidential, except with respect to authorized access through policy or by statutory authority. All pertinent files concerning companion and coworker information are stored and held in a safe and secure setting for a period of 7 years. All contractual files are held for a minimum of 7 years and all personnel and payroll are retained for a minimum of 4 years.

PROCEDURE

Use of the Cascadia communication systems must be lawful, ethical and consistent with the Cascadia's professional reputation, standards, policies and procedures. The Cascadia Society reserves the right to access, inspect, retrieve, read, copy, store, delete, distribute or disclose to others (including law enforcement authorities and courts) all communication systems data. This may be done without notice as considered appropriate by Cascadia. Cascadia coworkers adhere to a high standard of professionalism when using internal or external communication systems.

The following uses of Cascadia communication systems are prohibited:

- Personal or recreational use,
- Violation of computer integrity,
- Unauthorized tampering with computer hardware or software,
- Illegal, immoral, or unethical uses,
- Distribution of material protected by confidentiality, copyright, or trademark,
- Use of sounds or visuals which might be disruptive to others,
- Sending, receiving, or accessing messages, images or material that is racist, objectionable, abusive, pornographic, obscene, sexist, harassing or provocative, including adult-oriented websites or new groups,
- Defamatory, derogatory, or false messages,
- Unauthorized political activities, solicitation of funds, advertising,
- To perpetrate any form of harassment,
- Intentionally disrupting or "hacking" the IT systems of this or any other organization or individual,
- To perform work for other contractors or other employers,

- Commercial, or business uses,
- Unsecured disclosure of confidential or privileged information,
- Unauthorized use of data encryption,
- Uses that may compromise the system integrity or degrade system performance.
- Communication systems are not for personal purposes, except in emergency situations or authorized by management. This includes telephone, email, Internet, and fax.
- Personal cell phones are not to be used during working hours except for Cascadia operations or in the event of an emergency.
- Coworkers and companions we support are not responsible for costs of maintaining Cascadia communication systems.

DEFINITIONS

Information Technology (IT) Resources: Refers to all hardware, software, networks and data owned by or licensed to, and operated by The Cascadia Society for Social Working

ACCEPTABLE USE

Computers that are in programs and locations where Cascadia companions reside or where Cascadia business is conducted are to be used in a manner that is consistent with the Code of Ethics and Confidential Policy. All employees/contractors/practicum students are expected to role model computer in accordance with the Code of Ethics.

Coworkers, contactors, interns and volunteers expected to use computers at their home office, or otherwise (as in the use of laptops) to communicate through e-mails, the Internet, and other technological avenues (e.g. text messaging) are expected to do so in a manner that is consistent with the Code of Ethics and Confidential Policy.

For all coworkers, contractors, interns and volunteers of the Cascadia, it is only acceptable to use the Cascadia's IT resources for purposes that are approved by the management group and are directly related to the mission and business of the society.

UNACCEPTABLE USE

If a coworker, contractor, intern or volunteer violates any of the acceptable use provisions, applicable provincial and federal laws, or written policies, they will be in violation of their contract or terms of employment. Termination of the contract or disciplinary action may ensue.

If violations constitute a criminal offence, legal action may result. The following are selected examples of unacceptable uses of IT resources. They are not meant to comprise a complete or exhaustive list and may be amended at any time without notice.

EXPECTATION OF PRIVACY

All data transmitted; whether sent or received including any stored data is considered the exclusive property of Cascadia.

DATA BACKUP / RECOVERY

INTEGRITY

All files on Cascadia's network are backed up daily on Google Drive; Cascadia database is backed up every second day on a USB stick. Once a month both systems are backed up on one of two external hard drives – one kept on site and one-off site and are rotated each month. Cascadia's bookkeeping is contracted off site. The bookkeeper uses Cascadia's laptop, QuickBooks is backed up on one of two USB sticks - one kept on site and one-off site. Please note: All documents sent to an external source i.e. medical physician or community professional are to be sent via fax.

BUSINESS CONTINUITY/DISASTER RECOVERY

EMERGENCY PREPAREDNESS

All data collected and information networks and systems follow provincial and federal security, confidentially and emergency preparedness practices that involves ensuring the integrity of software, hardware, data and all operating systems.

VIRUS PROTECTION

Virus protection is employed on all Cascadia IT resources (at all times) and updated daily to Google Drive to ensure every effort is made to limit the collection of information that is corrupt or damaged.

SECURITY

No IT services shall be provided to external organizations or individuals without the express permission of the management team. This includes file sharing, Web services, and Internet access.

Passwords that grant any access to the Cascadia IT resources from inside o**r** outside the society will be at least eight (8) characters in length and contain a combination of letters in upper and lower case, and numbers. Computers are set to automatically lock their screens within 10 minutes of inactivity and requiring a password to open. Administration team computers are located in secure areas inaccessible by clients.

ACCESS MANAGEMENT

Access to all computer/technology services is password protected and specific to staff roles/responsibilities. The leadership team determine access to information not related or beyond a coworkers' job description or responsibilities. All computers have an admin password and a guest option that does not allow access to files.

AUDIT CAPABILITIES

Computer use/access is audited randomly by checking the access log and the history on computer browsers. The Business Director monitors and audits all system use.

DATA EXPORT AND TRANSFER CAPABILITIES

Any and all data related to companion, operational or program is not permitted to be removed from Cascadia premises without express permission/authorization.

DECOMMISSIONING PHYSICAL HARDWARE AND DATA DESTRUCTION

When physical hardware is decommissioned the hard drive in the unit is formatted to erase all previous data before the hardware is reassigned within the facility. Should the hardware be sent outside the facility for recycling the hard drive is removed and either physically destroyed or locked in the Administration office before the hardware leaves the facility.

PROTECTION FROM MALICIOUS ACTIVITY
This is performed by limiting access to critical systems and through anti-virus and monitoring software.

REMOTE ACCESS AND SUPPORT
Remote access to the network is restricted to the Leadership Team and IT Supervisor only.

UPDATE, CONFIGURATION MANAGEMENT AND CHANGE CONTROL
Company computers are set to automatically update during the overnight hours to minimize impact to the users.

ETIQUETTE GUIDELINES
Coworkers, contractors and volunteers will follow Internet and E-mail etiquette guidelines:

- Be always polite
- Do not use vulgar, obscene language or sarcasm.
- Use caution when revealing your address or phone number (and do not reveal the address or phone number of others without their explicit permission).
- Respond to messages or requests promptly.
- Do not send messages of a confidential or personal nature outside of the society.
- Abide by generally accepted rules of network etiquette.

INTERNET AND E-MAIL ACCESS
Internet access is expected within the Cascadia programs in order to promote a higher level of service delivery.

Personal use must be of an incidental nature and must not interfere with business activities or work schedules, must not involve solicitation, must not be associated with any outside business activity, and must not potentially embarrass Cascadia, its coworkers, contractors, volunteers, interns or companions.

Internet communications generated from Cascadia computers are considered the property of the Cascadia; users shall not have the expectation that their communications are private. 'Chat lines' are not permitted.

PURPOSE
The purpose of these policies is to outline the responsibilities of the Cascadia, and its coworkers, contractors, interns and volunteers regarding the society's Information Technology resources. In addition to these policies, federal and provincial laws or regulations may be in force and may take precedence over them.

- To ensure the integrity of Cascadia's computer network.
- To provide the parameters for computer use by Cascadia coworkers, contractors, interns and volunteers.

PROCEDURE

Technology

- The Cascadia's IT resources will be used by all coworkers, contractors, interns, and volunteers in a responsible manner that reflects these and Cascadia's other policies and procedures.
- Ensure the society's data, including medical, companion, financial and coworker/contractor/intern/volunteer records are kept confidential according to the procedures defined in the society's policy and procedure manual.
- Ensure that the headers of e-mail messages that are sent to groups do not reveal the private email addresses of the individual recipients.
- On computers owned by Cascadia it is expected that people will only use software and hardware that is provided and/or approved by the Leadership Team.
- Adhere to all software license provisions.
- Never transfer the society's data to a computer that is not owned by the society unless authorized to do so.
- Adhere to copyright restrictions on all materials obtained from outside of the Cascadia.
- Safeguard the society's intellectual property including, but not limited to, publications and Websites.
- Requests for repairs and maintenance to a computer system must first be approved by the management team and then be forwarded to the Finance & Operations Manager for follow up.
- Use only their own identity while using the society's IT resources.
- Conduct their electronic communications in a professional manner following the *Internet and E-mail etiquette guidelines as outlined above*.
- If a coworkers, contractors and volunteers identify a security problem, it is to be communicated to all who may be affected and the Finance & Operations Manager immediately.
- Do not show or identify a security problem to others outside the Cascadia.
- Avoid unnecessary subscriptions to mail/new sites even if they are free.
- E-mail attachments from unknown sources are to be deleted without being opened.
- It is safer to never download anything from the web without prior approval from the management team.
- Will open any new Cascadia on-line accts without direct permission or authorization.

Standards associated with this policy: 1) 1.J.1 and 2) 1.J.3

RESPONSIBILITY OF: All Coworkers, Contractors, Interns and Volunteers
MONITORED BY: Leadership Team; Business Director