Electronic Records Management

POLICY

Documentation produced or stored electronically must meet all applicable legislation Guidelines. Cascadia Society establishes and maintains a records management system, which complies with the guidelines of all applicable provincial and federal legislation. Electronic files and records are held secure and confidential, except with respect to authorized access through policy or by statutory authority. All pertinent files concerning coworkers and companions are stored electronically for a specified period of time. Confidential electronic records of coworkers and companions are backed up on the network and stored off site. Creation, access, removal, or destruction of records or files adheres to established policies and procedures.

PROCEDURES

DESTRUCTION OR DISPOSAL OF FILES

Material deemed to be ready for destruction is deleted from the system. Only designated files can be deleted.

LOCATION OF FILES

Coworker & companion files are kept in a secure database. Access is controlled through permission rights. Coworker and companion financial files are password protected by the Leadership Team. Files are backed up on Cascadia Society data system and additional stored at an appropriate off-site facility.

REVIEW

Electronic records are reviewed as needed by authorized personnel. Archival of removed material follows established guidelines to ensure the security and safety of all confidential information.

SECURITY

Electronic files are password protected. The Leadership Team with the Administration manages all file passwords and ensures files are regularly backed up on site. Designated leadership and administration coworkers have access to file information. All hardware i.e. USB sticks used to access material is secure and complies with statutory requirements. Designated leadership and administration coworkers are responsible for the opening, maintenance, closure, and disposal of files related to the operation of programs; companion reporting, site maintenance and incident reports. Removal of records from programs, without adherence to established policies, is strictly forbidden.

Standards associated with this policy: 1) 1.E.1, 2) 1.E.3 and 3) 1.I.4

RESPONSIBILITY OF: Business Director
MONITORED BY: Leadership Team