USE OF ELECTRONIC COMMUNICATION SYSTEMS BPE 2

INTENT

To provide employees, students and volunteers with instructions as to the appropriate use of the Society's electronic communication systems and equipment with the goals of safeguarding personal and confidential information and reducing personal risk.

POLICY

Use of Sunshine Coast Community Services Society's electronic communication systems must be lawful, ethical and consistent with the Society's professional standards. When you use the Society's electronic communication systems there is no guarantee of personal privacy. The computer and telephone systems are owned and managed by the Society and therefore we reserve the right to access, retrieve or review all information, including communications by employees when deemed necessary and when required by law. Use of the Society's electronic systems that contravenes the policy or procedures as laid out will result in disciplinary action up to and including termination of employment.

PROCEDURE

The following uses of SCCSS electronic communication systems are prohibited:

1. Sending, receiving or accessing messages, images or other materials that contravene the Human Rights Code of BC, or are offensive, objectionable, abusive or harassing.
2. Illegal, unethical or immoral uses including hacking or spoofing.
3. Distributing email chain letters or junk mail.
4. Sending defamatory, derogatory, false or libellous messages.
5. Other commercial or business uses.
6. Political activities, solicitation of funds, or advertising goods and services.
7. Uses that infringe copyright.
8. Unsecured disclosure of confidential information.
9. Unauthorized access to other users' email, data or communications.
10. Downloading unauthorized software.
11. Introducing viruses or spyware.
12. Uses that may compromise system integrity or degrade system performance

Server access is restricted to authorized users with assigned administrative permissions (i.e. digital rights). Attempts to circumvent these permissions will result in discipline up to, and including termination.

This list does not limit the right of Community Services to consider other activities outside of directly work-related activities as unacceptable.

COMPUTER SYSTEMS

Computer systems include the dedicated server, laptop computers, desktop work stations and portable devices, and computer users must adhere to the following:

- Approved licensed software and hardware is installed and maintained by third-party supplied IT services approved and contracted by the Society. Unauthorized installations of computer hardware and software by employees is prohibited.

SECURITY

1. Firewalls and virus protection software applications and update schedules may not be altered or disabled.
2. Secure confidential information by using passwords and other means as required, e.g. firewalls, encryption. Passwords may not be shared.
3.
4. All PC's including monitors must be logged off whenever an employee leaves his/her office.

ELECTRONIC CLIENT RECORDS (ECR)

For programs that have electronic client records (ECR) the following practices will apply:

1. The ECR is a secure and encrypted web based system for storage of client records. Files can only be accessed using a password. Employees are not to share passwords.
2. The preference is for the ECR to be accessed at the employees assigned work site or other Sunshine Coast Community Services location.
3. This will not always be possible especially for employees working only a few hours per week supporting clients in the community. With direct supervisor's knowledge and permission employees may access the system from a location other than a work site. Managers, supervisors and Coordinators will review confidentiality practices with employees when they request permission to access the system off site.
4. The ECR is not to be accessed from any public spaces such as recreation centres, libraries, schools, coffee shops, restaurants or stores. When accessing the ECR it must always be accessed using a password-protected network.
5. When accessing the ECR from a location such as the employee's home employees must ensure that no one but the employee is able to view the website and files and that clients cannot view or access any personal or confidential information that is not their own.
6. Employees must always treat the ECR with the same level of confidentiality they would treat any documentation regarding a client or client record.
7. Employees must not leave their device open on the ECR and unattended.
8. When employees are using their own personal devices they must not store any client documents on their own personal devices. All information must be stored in the ECR client file.

EMAIL GUIDELINES

1. Employees must not attempt to read another person's email unless authorized.
2. Email transmissions are not secure and discretion should be used in relaying confidential information.
3. Employees are encouraged to create separate signature files for each of their programs or departments and use them in email communications that are sent from SCCSS accounts. The text of the official signature file must list job title, department and telephone or fax number. An email is an official record if it was created or received as part of the normal business of SCCSS and contains information of significance to SCCSS.

4. Due to potential risk, employees may not enable auto-forwarders to a non-SCCSS email. Likewise, the reverse is prohibited.
5. An email disclaimer must appear on all SCCSS email correspondence.

VOICE MAIL

1. Employees will ensure their recorded voice mail messages are appropriate, informative and timely
2. Employees are responsible for the security of their account and password and precautions must be taken to prevent unauthorized access to mail boxes.

CELLULAR PHONES

1. Staff will maintain the phone in a manner conducive to appropriate use, e.g. keep batteries charged and ensure that the phone is stored safely and securely.
2. Clients are permitted to use the cell phone when necessary, but only under staff supervision.
3. Staff are prohibited from using cell phones while they are driving.
4. Cell phones that are the property of Sunshine Coast Community Services Society must be returned upon termination of employment with the agency, or upon request.
5. Cellular transmissions are not secure and discretion should be used in relaying confidential information.
6. The cost of using personal cell phones for work purposes will be reimbursed as an expense, following approval by the supervisor.

REFERENCE HR BPE 2A – CELL PHONE EXPENSE

PERSONAL USE

1. Communication systems may be used for very limited personal purposes provided that those uses do not compromise the integrity and efficiency of the Society's business and communications systems, its professionalism or its reputation. Additional charges incurred for personal use will be reimbursed to the Society.

2. Staff using personally-owned computers connected to the SCCSS network, email system, server or ECR, must take measures to achieve effective virus detection and prevention and must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

PASSWORDS

All passwords for computer systems, emails, and voice mail will be filed with the Facilities Manager who will maintain this information in a secure, confidential storage place.

AGREEMENT

All employees or contractors who have been granted the right to use the company's electronic systems are required to sign this agreement confirming their understanding and acceptance of this policy.

SOCIAL MEDIA

REFERENCE HR C6.1 Employee Conduct - Social Media

ASSET MANAGEMENT/DISPOSAL OF ASSETS
REFERENCE HR AP8 Asset Management

EFFECTIVE: Dec. 1, 2015	**APPROVED BY: Executive Director**	
REPLACES: April 1, 2014	**MONITORING: Executive Director**	**FREQUENCY: Annually**