PRINCE GEORGE
HOSPICE
PALLIATIVE CARE
SOCIETY

INFORMATION TECHNOLOGY (IT)
Policies and Procedures

For Employees and Volunteers

Contents

The IT Policies and Procedures will be reviewed every two years by IT Support and confirmed by the Executive Director.

Next review date: 2023-02-01

	IT 9.00
Policy:	**System Security and Safety Measures**
Person Responsible:	**Executive Director**
Date Created:	September 2003
Last Revised:	February 2021

Policy:

All PGHPCS files and documents must be backed up regularly and stored in multiple locations. Users are encouraged to keep all files on the server for automatic backup and apply all security and safety measures to protect Society's hardware and software.

Procedure:

1) The Society's network is backed up daily, and offsite backups are stored with encryption over the cloud on Ascentech servers.
2) Data stored on offsite PC drives, i.e., at home locations, are not routinely backed up. As a result, important data and applications could be lost. Offsite data should be stored in a OneDrive folder cloud synced to the user's work computer. No confidential information should be kept in OneDrive.
3) All data disks, portable drives (including jump drives), and files entering the Society network should be scanned for viruses. Unfamiliar drives, i.e., a randomly found drive, must NEVER be plugged into society computers.
4) Users are encouraged to log off their computer or turn the computer off before leaving. Users should lock their computers when they are away from the computer for an extended period.
5) Avoid eating, drinking, and the placement of any hazardous substance on or near computer hardware.
6) Files and communications created in the normal course of the Society's business and stored on the Society's computers or storage media are the Society's property.

Policy:	**IT 9.01** **Confidentiality**
Person Responsible:	**Executive Director**
Date Created:	September 2003
Last Revised:	February 2021

Policy:

All users will respect the rights of other users to the security of files and confidentiality of data. All information stored in the Society system(s) will be deemed confidential.

Procedure:

1) All Society policies and all federal and provincial laws and legislation regarding confidentiality and privacy will be followed.

2) Users of Society computer systems will be assigned passwords for their accounts. The account holder is responsible for the proper use of the account, including proper password protection and ensuring that only he/she has access to the account.

3) All files containing confidential information shall not be removed from PGHPCS servers or transported through portable data drives except in emergencies. In which case, the drive shall be purged after use by IT support.

4) The IT support will monitor all systems to ensure system integrity and system performance. During this process, they may have access to certain information deemed confidential. Every effort will be made to ensure user privacy; however, if violations are discovered, they will be reported immediately.

Policy:	**IT 9.02** **Use of Electronic Mail**
Person Responsible:	**Executive Director**
Date Created:	September 2003
Last Revised:	February 2021

Policy:

The Society will assign email accounts to all employees to conduct work-related business and correspondence.

Procedure:

1) Should an employee provide another person with access to their account, they will be responsible for the individual's actions using their account.

2) The email system is not to be used to solicit for commercial ventures, religious or political causes, outside Society's, or other non-job-related solicitations.

3) Using the email system for job-related solicitations, users will ensure that they have proper consent to send to all external recipients. This may include express consent or implied consent as defined in the *Federal Fighting Internet and Wireless Spam Act*. Constant Contact will be used for all external mass emails

4) The system is not be used to create any offensive or disruptive messages. Among those which could be 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 origins, or disability.

5) Employees may not use their Society email address in conjunction with any online service, product, or website that is not directly related to their work for the Society.

6) All email usage must meet the highest ethical, professional, and legal conduct and personal integrity.

7) Information on the system will not be deemed personal or private. Information sent by employees via the electronic mail system may be used in legal proceedings

8) Email storage capacity per account is **50GB.** Exceeding this limit will automatically disable the account.

Policy:	**IT 9.03** **Creation and Use of Personal Images**
Person Responsible:	**Executive Director**
Date Created:	September 2003
Last Revised:	February 2021

Policy:

The use of image capture devices creates a wide variety of challenges for PGHPCS, especially around the areas of consent and confidentiality. Images may only be stored on PGHPCS computers or other storage media if they are for the agency's valid operational use and are considered confidential information. Employees are encouraged to become familiar with the various pieces of legislation involved in the handling of confidential and sensitive material

Definitions:

Images – Images include photographs, digital photographs, video footage, or other images created through the use of an image capture device. Images may be physical objects (such as photographs) or electronic files (in whatever image encoding format, including streaming images). Images in any form are considered "documents" for all purposes, legal and informal, including those relating to Policy HR 5.12 Privacy and Confidentiality.

Image Capture Device – Image capture devices include all devices that can capture a visual image or series of images, whether still images or video images. These devices include still cameras (reflective, digital, and all other forms), video cameras, digital camcorders, cellular phones with integrated cameras, cameras hooked up to or integrated into a computer system ("webcam"), and any other such device.

Public Website – The PGHPCS public website is located at www.pghpcs.ca

Note: This policy is intended to be used in conjunction with the Freedom of Information and the Protection of Privacy Act of British Columbia (FOIPPA), the BC Privacy Act, and the Federal Personal Information Protection and Electronic Documents Act (PIPEDA). Where this policy conflicts with any of these Acts or any subsequent Act(s) that supersedes (replaces) any of these Acts, the Act will take precedence.