Acceptable Use Policy

Sprott Shaw College's (SSC) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to SSC's established culture of openness, trust, and integrity. SSC is committed to protecting its employees, students, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet use are the property of SSC. These systems are to be used for business and academic purposes in serving the interests of the company and students in the course of normal operations.

Effective security is a team effort involving the participation and support of every SSC employee, student and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computers and other technological equipment at SSC. These rules are in place to protect the employees, students, and SSC. Inappropriate use exposes SSC to risks including virus attacks, compromise of network systems and services, confidentiality, and other legal issues.

POLICY

General Use and Ownership

- Users should be aware that the data they create on SSC's Technology remains the property of SSC. Because of the need to protect SSC's network, management cannot guarantee the confidentiality of information stored on any network device belonging to SSC.
- Students are responsible for exercising good judgment regarding the reasonableness of any use of SSC Technology.
- By using SSC Technology, it is hereby acknowledged that for business, employment, security, and network maintenance reasons, authorized individuals within SSC may monitor SSC Technology at any time.
- SSC reserves the right to audit SSC Technology to ensure compliance with this policy.
- SSC reserves the right to block or re-direct inappropriate web sites at its sole discretion.
- Use of any SSC Technology is restricted to students who are actively working or enrolled at SSC. Priority is given to those students who are scheduled for a specific time period to train on the computer systems. Any student who is not scheduled to use a computer may not enter the computer lab without having booked a set time period in advance of when they need access. Exceptions are made at the discretion of the computer instructor or Director.

- Students that bring in their own personal equipment including but not limited to computers, smart phones and notebooks are responsible for their own equipment. Such equipment must comply with acceptable use guidelines including use and anti-virus protection. At no time does SSC assume any responsibility for either lost or stolen equipment or damage to equipment or data files stored on such equipment.
- Wireless network access is provided "as is" with no express warranties of service availability nor security. Students assume all responsibility for the use of such services.

Security and Proprietary Information

- The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to company privacy, corporate strategies, competitor sensitivity, trade secrets, curriculum, specifications, customer lists, student lists, and research data.
- Keep passwords secure and do not share accounts except those accounts specifically indented for shared access such as student logon accounts. Authorized users are responsible for the security of their passwords and accounts.
- All computers used by students that are connected to the SSC Internet/Intranet/Extranet, shall be continually executing approved virus-scanning software.
- All storage media used on SSC Technology will be subject to random virus and malware scanning and usage logging. Any storage media device which is suspected of being infected with a computer virus or other form of malicious software may have files deleted, damaged, or the device or item may be immediately destroyed. If this is the case, then SSC shall not be held responsible for restoring, repairing, or replacing affected files or such devices. SSC shall not be held responsible for any personal device or storage media device infected by any computer viruses or malicious computer programs, including but not limited to loss of data or programming, regardless of means of digital infection, computer use is at own risk.
- Employees and students must use extreme caution when opening e-mail attachments received from unknown senders which may contain viruses, e-mail bombs, Trojan horse, or other forms of malicious code.
- Users will be required to authenticate using a MFA approved by Sprott Shaw in order to access certain Sprott Shaw Technology. Users shall not share or permit any other individual to use their MFA method.

To safeguard your personal information and financial assets, all users must remain vigilant against phishing attempts, spam messages, and fraudulent email communications. The following guidelines are strictly enforced:

- Do Not Share Sensitive Information: Under no circumstances should you disclose login credentials, account numbers, or personally identifiable information (PII) in response to unsolicited messages.

- Be Cautious of Email Requests: Emails requesting changes to account details or prompting the transfer of funds—especially those claiming urgency or offering incentives—should be treated with suspicion. Always verify such requests through official channels.
- Verify Before Acting: If you receive a message that appears to be from this organization asking you to update account information or send funds, confirm its legitimacy by contacting us directly via approved communication methods.
- Report Suspicious Activity: Immediately report any suspicious messages or phishing attempts to our IT team. Timely reporting helps prevent further abuse and protects others in the organization.
- Use Strong Authentication: All users are encouraged to enable multi-factor authentication (MFA) and to regularly update passwords to enhance account security.

Remember: We will never ask for sensitive account details or direct fund transfers via unsolicited email.

Unacceptable Use

The following activities are, in general, prohibited. Under no circumstances is a student of SSC authorized to engage in any activity that is illegal under local, provincial, federal, or international law while utilizing SSC Technology.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SSC students.
- Visiting any objectionable Internet site, including, but not limited to, pornography or advocacy of illegal actions of any form, sites which negatively depict race, sex or creed, violence or any site which violates the rights of another human being.
- Unauthorized copying or downloading of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, internet or other copyrighted sources, copyrighted music, videos, and movies nor the installation of any copyrighted software for which SSC or the end user does not have an active license is strictly prohibited.

- Students are not authorized to download and/or install any software on any SSC Technology including but not limited to freeware, shareware, games, helpers, and tool bars or point to point sharing programs such as Bit Torrent.
- Tampering with any data files, program files, or software defaults on any computer system.
- Exporting software, technical information, encryption software or Technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to the export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs or any other malicious code).
- Revealing your account password to others or allowing use of your account by others except shared employee and student accounts. This includes family and other household members when work is being done at home.
- Using SSC Technology to actively engage in procuring or transmitting material that is in violation of any laws or regulations in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any SSC account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the student is not an intended recipient or logging into a server or account that the student is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, port scanning or security scanning, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious or non-malicious purposes.
- Executing any form of network monitoring which will intercept data not intended for the student.
- Circumventing user authentication or security of any computer, server, network, or logon account.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/ Extranet.
- Providing information about, or lists of, SSC employees or students to parties outside SSC.
- Personal use of SSC Technology shall not interfere with one’s work or studies and is restricted to non-working hours and breaks.

Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.

- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within SSC networks of other Internet/ Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SSC or connected via SSC network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups.

Blogging

- Blogging by students, whether using SSC Technology or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of SSC Technology to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate this or other SSC policies, is not detrimental to SSC best interests. Blogging using SSC Technology is subject to monitoring.
- Students shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of SSC and/or any of its employees or students. Students are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by SSC non-discrimination and anti-harassment policies.
- Students may also not attribute personal statements, opinions or beliefs to SSC when engaged in blogging. If a student is expressing their beliefs and/or opinions in blogs, the student may not, expressly, or implicitly, represent themselves as a representative of SSC.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, SSC's trademarks, logos, and any other SSC's intellectual property may also not be used in connection with any blogging activity.

Social Networking

- Any use of social networking, including but not limited to Facebook, LinkedIn, Twitter, Instagram, Snapchat and TikTok shall not interfere with work and school commitments.
- Students are legally liable for anything they write or present online. Users of SSC's Technology are responsible for any unauthorized charges, fees, costs, damages or resulting injuries from their use of SSC Technology.
- Students may be disciplined by SSC for commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment, or might otherwise result in legal action.
- Most individuals view their personal email and social networking pages as private. However, students should be aware that any of the information or communications posted on their email or social networking sites can potentially be accessed by current or potential employers, co-workers, agencies, other students or employees, clients, employer's competitors, government and law enforcement agencies and others outside your trusted network.

- Depending on the privacy settings set by the individual user, personal information and communications posted on a social networking site can be read by unintended people. Above mentioned confidentiality and privacy rules apply to social networking.

Enforcement

Any student found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or studies.

Definitions

"Blogging" means writing or publishing a blog, being a personal online journal that is frequently updated and intended for general public consumption.

"Multi-Factor Authentication (MFA)" means a method of verifying a person's identity in order to allow access to a digital service or system, requiring one or more proofof identity in addition to a password or PIN, such as a code texted to a phone or a response to an application.

"Sprott Shaw College Technology" means any electronic device, service or system designed or used to assist in extending human potential (including but not limited to computers, mobile communication devices, cameras, social networking sites, email and voice services, school networks, etc.) owned, leased and/or operated by SSC.

"Spam" means unauthorized and/or unsolicited electronic mass mailings.

Note: The students Sprott Shaw email account may be disabled for violation of the College Acceptable Use policies and/or withdrawal/dismissal from the College.