Policy OP 03:
Information Technology

1.0 Purpose

The purpose of this policy is to define the acceptable use of Information Technology (IT) resources in support of the mission of SKG. It builds on the principles of accountability, transparency, privacy, and fairness, to support a functional environment for work and study in which these resources are protected.

2.0 Application

This policy applies to anyone who uses or accesses any IT resource belonging to, under the control or in the custody of SKG. This includes employees, students, and any one else who has been granted authorization by SKG to use its IT resources.

3.0 Definitions

“Account” means any username, access code, password, PIN, token, credential, or other authentication which has been assigned to authorized users to use any IT resource.

“Authorized” means specific access rights granted in accordance with SKG policies.

“Authorized user” means a member of the SKG community, who is an employee, student, alumni, associate, or other individual who has been granted specific rights by SKG, or someone delegated in accordance with SKG policies to use any IT resource of SKG.

“Community standards” means behaviour or material which the average member of the SKG community would reasonably tolerate.

“Director of Operations” means the senior executive appointed by SKG’s board of governors who is responsible for operations including information technology, regardless of the title of that position.

“Information Technology resource” and “IT resource” means any information, data, software, hardware, system, or network belonging to, under the control or in the custody of SKG, regardless of who administers it.

“Personal information” means recorded information about an identifiable individual, and as defined in federal and provincial privacy legislation.

“System administrator” means an individual responsible and authorized to establish or maintain and provide technical support for an SKG IT resource. A system administrator could be an SKG employee or contractor.

4.0 Policy

4.1 Acceptable use of IT resources

SKG authorizes members of its community to use its IT resources to fulfill and advance SKG's mission, including teaching, learning, research, service, community development, and administration of its programs and activities.

Authorized users must exercise good judgment in determining what is acceptable use of IT resources with due regard to this policy, other SKG policies and community standards. Some activities may be appropriate only in a specific context (for example, for academic and research purposes), while some are not appropriate in any context.

Authorized users shall take all reasonable steps (for example, password protection) to protect the confidentiality, integrity, and availability of IT resources.

A user is responsible for all activity originating from his or her account or other IT resource, regardless of who actually may be using the account or other IT resource.

Authorized users shall report encountered vulnerabilities to the Director of Operations. Failure to do so may constitute a breach of this policy.

Users are expected to give consideration to maximizing SKG's IT resources and to proper file management. Accumulation on the network of unnecessary, out-dated, or non-work-related files is discouraged.

Breach of acceptable use

Users shall not use IT resources in a way that that breaches appropriate use, unless a use is explicitly authorized by the Director of Operations.

A breach of acceptable use includes, but is not limited to:

- Use of an IT resource to create, store or transmit material that is in violation of the Criminal Code of Canada, or the Ontario Human Rights Code or any federal, provincial or municipal laws or regulations;
- Use of an IT resource in a threatening, discriminatory, or harassing manner;
- Viewing or using hateful, pornographic, or offensive material;
- Distributing or disseminating hateful, pornographic, or offensive material;
- Use of an IT resource that is in violation of any SKG policy;
- Allowing others to access your assigned personal account;
- Failure to exercise reasonable care in safeguarding accounts and information;
- Accessing someone else's personal account;
- Seeking information on passwords or information belonging to others;

- Falsifying or misrepresenting your identity;
- Copying, deleting, intercepting, or examining someone else's files, programs, or information without consent or authorization by SKG;
- Attempting to collect, use, or disclose, the personal information of others;
- Breaking or attempting to circumvent licensing or copyright provisions;
- Attempting to circumvent information security provisions or exploit vulnerabilities;
- Any interference with the ability of others to use IT resources, whether or not it is disruptive; and
- Using IT resources for unauthorized commercial purposes (see also the section of this policy addressing commercial use).

4.2 Personal use of SKG's IT resources

SKG permits limited personal use of these resources, provided this use does not violate any law, statute, or SKG policy.

Users who require a private means of computing and sending electronic communications should utilize a personal device unconnected to the SKG's IT network.

4.3 Commercial use of SKG's IT resources

Users may not make commercial use of SKG's IT resources, without the express prior approval of the Director of Operations.

Commercial use includes but is not limited to:

- Using an SKG email address in commercial correspondence,
- Distributing advertising material,
- Including click-through links or banner ads on a website hosted on SKG's network,
- Offering information or services for sale or personal gain,
- Operating a commercial server over SKG's network,
- Using SKG's network resources to provide computing services outside SKG's network or to provide any external computing service to the campus or wider community.

4.4 Privacy and personal information in IT resources

SKG respects the privacy of all users of its IT resources and uses reasonable efforts to maintain confidentiality of personal information.

Circumstances may arise in which such privacy cannot be maintained. Access to personal information may be granted to an authorized user, system administrator, or an agent of SKG to meet legitimate SKG business needs and operational requirements, investigate a possible

breach of this policy, or in the event that an authorized user is unavailable or has their access revoked.

Such access shall be approved by the Director of Operations.

4.5 SKG access to IT resources and information in them

SKG may audit, access, or restore any IT resource within its environment when it has reasonable grounds to suspect a breach of acceptable use or a possible violation of any law or SKG policy.

Such access shall be approved by the Director of Operations.

4.6 Consequences of breach of this policy

The Director of Operations may direct the locking or quarantining of an account or IT resource at the Director of Operations' sole discretion if the integrity or security of an IT resource is compromised or at risk.

The Director of Operations may initiate an investigation to address a concern about whether this policy has been breached.

If the Director of Operations determines that a user has breached the policy, and having regard to the seriousness and impact of the conduct, the Director of Operations may:

- Issue a warning;
- Apply conditions on access to or use of IT resources;
- Apply restrictions on access to or use of IT resources;
- Where the user is a student, refer the matter to academic discipline under SKG's policies on student conduct or academic integrity as applicable;
- Where the user is an employee, determine a disciplinary consequence up to and including dismissal; or
- Where conduct may have been criminal, refer the matter to the police.

5.0 Related Policies, Procedures & Documents

SKG's policies and procedures may be found here.

6.0 Responsible Officer

Director of Operations

7.0 Version history

Approved by:	Board
Original Approval Date:	March 28, 2023

Current Approval Date: March 28, 2023

Effective Date: March 28, 2023

SKG gratefully acknowledges that parts of this policy are patterned on those of the University of Guelph, Nipissing University, and OCAD University.