Code: H: Curriculum and Instruction

POLICY TITLE AND CODE

TECHNOLOGY ACCEPTABLE USE POLICY HBL

STATEMENT OF POLICY

The Greater Saskatoon Catholic Board of Education believes schools are a faith-based community adapting technology to enrich learning and promote excellence in education.

RATIONALE

The purpose of this policy is to detail the acceptable use of corporate Information Technology (IT) resources for the protection of all parties involved. Employees are granted access to technology in order to perform their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the division network. Since inappropriate use of division systems exposes Greater Saskatoon Catholic Schools (GSCS) to risk, it is important to specify exactly what is permitted and prohibited.

DEFINITIONS

1. **Blogging:** The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").

2. **Guideline:** Recommendations for implementing policies and standards.

3. **Instant Messaging:** A text-based computer application that allows two or more Internet-connected users to "chat" in real time.

4. **Peer-to-Peer (P2P) File Sharing:** A method of sharing files between directly between computers and users, instead of using a central server or file share, utilizing software that connects computers using the internet.

5. **Policy:** A set of principles intended to govern actions.

6. **Procedure:** Actions necessary to carry out policy or implement a standard**.**

7. **Remote Desktop Access:** Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

8. **Standard:** Required specifications that must be implemented to achieve policy compliance.

9. **Streaming Media:** Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

BELIEFS

1. Technology is an integral part of education.
2. All stakeholders are invited to have voice.
3. Students and teachers work to achieve curricular outcomes by adapting technology.
4. Professional development opportunities for teachers/staff are critical for effective integration of technology.
5. Technology must be student centered and used to empower students by developing skills to meet their diverse needs as global and digital citizens.

PROCEDURES

A. Monitoring and Privacy

GSCS reserves the right to monitor any and all use of the computer network. To ensure compliance with GSCS policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media. Users should not expect privacy when using the corporate network or GSCS resources.

B. Unacceptable Use

The following actions shall constitute unacceptable use of the division network. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. Employees may not use the division network and/or systems to:

1. Engage in activity that is illegal under the Criminal Code, local, provincial, or international law.

2. Engage in any activities that may cause embarrassment, damage the reputation, or cause other harm to GSCS.

3. Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.

4. Engage in activities that cause disruption to the workplace environment or create a hostile workplace.

5. Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of the employee's job function.

6. Install or distribute unlicensed or "pirated" software.

7. Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

8. Engage in Peer-to-Peer (P2P) networking.

9. Stream media, unless for a job-related function.

10. Circumvent any security systems, authentication systems, user-based systems, or escalating privileges. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

C. Passwords

Solid password procedures are perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand process is essential.

In order to maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. Greater Saskatoon Catholic School employees will be required to change their password three times a year. For more information, see the Password Procedures document.

D. E-mail

1. Personal usage of GSCS email systems is permitted as long as:
   a. such usage does not negatively impact the corporate computer network, and
   b. such usage does not negatively impact the user's job performance.

2. The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, pyramid schemes and mass e-mails forwarding a personal agenda (i.e. promoting a personal business or selling items). This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.

3. The user is prohibited from attempting to impersonate another person.

4. External email is an insecure method of communication, and thus information that is considered confidential may not be sent via email, regardless of the recipient. For more detail, please see the Confidential Data Procedures and Data Classification Guidelines documents.

5. The GSCS e-mail system is not designed to transfer large files and as such, emails should not contain attachments of excessive file size.

6. For more detail, please see the Email Procedures document.

E. Confidentiality

Confidential data is typically the data that holds the most value to Greater Saskatoon Catholic Schools (GSCS). Often, confidential data is valuable to others as well, and thus can carry greater risk than general GSCS data.

Confidential data should not be:

1. Shared or disclosed in any manner to non-employees of GSCS.

2. Should not be posted on the Internet or any publicly accessible systems.

3. Should not be transferred in any insecure manner.

Please note that this is only a brief overview of how to handle confidential data, and that other policies, procedures and/or guidelines may refer to the proper use of this information in more detail. For more detail, please see the Confidential Data Procedures, Student Records Policy, or Student Records Guidelines.

F. Network Access

The user should take reasonable efforts to avoid accessing network data, files, and information that are not within the scope of his or her job function. The ability to access information does not imply permission to use this access.

G. Network Devices

In order to ensure the security of the GSCS network, and all users connected to the network, all devices attached to the network must meet minimum security requirements. For more detail, please see the Networked Devices Standards document.

H. Social Media

Blogging and/or social networking are allowed from the corporate computer network provided that:

1. It is done in a professional and responsible manner.

2. Confidential data is not disclosed.

3. It does not impact the user's job performance.

4. No information detrimental to GSCS is published.

The user assumes all risks associated with blogging and/or social networking. Instant messaging is allowed such that it follows procedures on disclosure of confidential data and does not negatively impact the user's job function.

I. Web Browsing

The world wide web is a public domain. Users can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. Employees must use the Internet at his or her own risk. GSCS is not responsible for any information that the user views, reads, or downloads from the Internet.

GSCS recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of GSCS computer systems to access the Internet is permitted as long as such usage follows procedures elsewhere in this document and does not have a detrimental effect on GSCS or the user's job performance.

J. Copyright Infringement

Division computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of the acceptable use policy, if done without permission of the copyright owner:

1. Copying and sharing images, music, movies, or other copyrighted material using Peer-to-Peer (P2P) file sharing or unlicensed CD's and DVD's.

2. Posting or plagiarizing copyrighted material.

3. Downloading copyrighted files which the employee has not already legally procured.

This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above. For more detailed information, the access copyright website, www.accesscopyright.ca/ is useful in addressing specific questions. An electronic copy of Copyright Matters: Some Key Questions and Answers for Teachers is available at:

http://www.cmec.ca/Publications/Lists/Publications/Attachments/12/copyrightmatters.pdf

K. Remote Desktop Access

Use of non-GSCS-supplied remote desktop software and/or services (such as Citrix, VNC, GoToMyPC, etc.) is prohibited. For more detail, please see the Remote Access Standards document.

L. Non-GSCS-Owned Equipment

The user must obtain written permission from the Manager of IT Services before installing outside or non-GSCS-provided computer systems on the GSCS network. Once this permission is obtained, and dependent on any conditions granted along with such permission, the user can only connect a non-GSCS-owned system to the non-CommunityNet wireless network (Guest Wireless Network). Precautions must be taken to ensure viruses, Trojans, worms, malware, spyware, and other undesirable security risks are not introduced onto the GSCS network. For more detail, please see the Wireless Access Standards document.

M. Personal Storage Media

GSCS does not restrict the use of personal storage media, which includes but is not limited to: USB or flash drives, external hard drives, personal music/media players, and CD/DVD writers, on the corporate network provided that guidelines for data confidentiality are followed. The user must take reasonable precautions to ensure viruses, Trojans, worms, malware, spyware, and other undesirable security risks are not introduced onto GSCS network. Use of personal storage media must conform to the Mobile Device Procedures document.

N. Software Installation

Proof of ownership will allow IT Services to install non-GSCS-supplied software after it has been approved by the Educational Technology Coordinator and/or Consultant. Please note that numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance.

O. Reporting of Security Incident

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor. Examples of incidents that require notification include:

1. Suspected compromise of login credentials (username, password, etc.).

2. Suspected virus/malware/Trojan infection.

3. Loss or theft of any device that contains GSCS information.

4. Any attempt by any person to obtain a user's password over the telephone or by email.

5. Any other suspicious event that may impact GSCS's information security.

P. Enforcement

This policy will be enforced by Superintendents of Education. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of GSCS property (physical or intellectual) are suspected, GSCS may report such activities to the applicable authorities.

REFERENCES

- Confidential Data Procedures
- Data Classification Guidelines
- Email Procedures
- Student Records Policy
- Student Records Guidelines
- Networked Devices Standards
- Remote Access Standards
- Wireless Access Standards
- Mobile Device Procedures
- Password Procedures

DATE APPROVED

January 7, 2013

DATE EFFECTIVE

January 7, 2013