Administrative Procedure 640

RESPONSIBLE USE OF TECHNOLOGY

Background

The Division supports and encourages the use of technology to enhance and facilitate student learning. Our goal is to ensure that interaction with technology contributes positively to the work and learning environments at school and in the community.

Digital Citizenship is the generally accepted behaviour of responsible citizenship carried over to online environments.

Procedures

1. The Superintendent ensures that effective, fair and prudent procedures exist to monitor and filter content and/or services distributed through those devices owned and operated by the Division, including:
   - 1.1 The Division's electronic network;
   - 1.2 The Division's email system;
   - 1.3 The Division's social media accounts; and
   - 1.4 All related digital or electronic applications considered to be Division property or Division digital resources.
2. Use of the Division's digital systems and devices, as well as the Division associated web services and social media for illegal purposes, including harassing behaviour, is strictly prohibited and shall lead to disciplinary action up to and including termination.
3. For the purpose of ensuring responsible use, the Division reserves the right to monitor any Internet, text and communication activity occurring on its hardware, software, equipment, cell phones, email accounts, and Division associated web services and social media.
4. Individuals using the Division's hardware, software, equipment, and accounts to access the Internet, network and applications are subject to having activities reviewed by administration.
5. Use of the Division's digital and Internet resources, network or equipment implies the user's consent to monitoring for security purposes.
   - 5.1 All users covered by this administrative procedure are to bear in mind that

Internet sessions and digital communications are likely not private.

6. With respect to Responsible Use

6.1 Employees, students and volunteers of the Division shall:

6.1.1 Demonstrate self-respect and sensible self-protection;

6.1.2 Take responsibility for actions when posting or viewing online information and images;

6.1.3 Use appropriate online etiquette;

6.1.4 Follow school and Division procedures and behaviour standards;

6.1.5 Respect and protect others, including:

6.1.5.1 Obtaining permission of all individuals before sharing or posting any information about them;

6.1.5.2 Obtaining permission from all individuals before sharing commonly created electronic data;

6.1.6 Follow applicable *Freedom of Information and Protection of Privacy Act* (FOIP) regulations when sharing or posting information;

6.1.7 Demonstrate an understanding that social media used for educational purposes is an extension of the classroom;

6.1.8 Take full responsibility for, and respectfully use, any technology available to them within the Division;

6.1.9 Act as an ambassador of the Division when using social media;

6.1.10 Use network bandwidth, file storage space and printers reasonably and only for Division related purposes;

6.1.11 Comply fully with federal or provincial laws or regulation, including copyright laws and fair use guidelines; and

6.1.12 Ensure that technology use is well within existing Division procedures (e.g. bandwidth limitations, network storage, etc.) and in alignment to the Division's vision, mission, goals, and reputation.

6.1.13 Protect the privacy of all students and staff by not making any recordings of any persons on school property without their consent with the exception of recordings made during public events. A public event is open to the general public, has been publicly announced and has been publicized in advance as such.

7. With respect to a duty to report

7.1 Staff and students shall:

7.1.1 Report abuse of technology or violations of any aspect of this procedure to their immediate supervisor, or to the Director of Information Technology or designate,

7.1.2 Moderate the publication of online content and seek prudent action when that content is deemed inappropriate as identified in this procedure; and

7.1.3 Report security or network problems to the Director of Information Technology or designate.

7.2 Employees, students and volunteers of the Division and any other individuals accessing Division owned technology SHALL NOT:

7.2.1 Access material deemed socially inappropriate;

7.2.2 Degrade or defame others in any manner;

7.2.3 Forward inappropriate materials or communication;

7.2.4 Utilize any Division technology for commercial, personal or financial gain;

7.2.5 Access or utilize technology for illegal purposes, such as theft, fraud, slander, libel, defamation of character, harassment (sexual and non-sexual), stalking, identity theft, online gambling, spreading viruses, spamming, impersonation, intimidation, and plagiarism/copyright infringement;

7.2.6 Copy, destroy, or alter any data, documentation, or other information that belongs to the Division or any other business entity without authorization;

7.2.7 Download unreasonably large files that may hinder network performance or in any way interfere with others' usage;

7.2.8 Access, download, or print any content that exceeds the bounds of good taste and moral values (i.e. pornography);

7.2.9 Engage in any other online (including social media) activity that would in any way bring discredit, disrepute, or litigation upon the Division;

7.2.10 Engage in personal online commercial activities during periods of work, including offering services or products for sale or soliciting services or products from online providers;

7.2.11 Engage in any activity that could compromise the security of the Division host servers or computers;

7.2.12 Disclose, to any other person, one's password or the passwords of others; or

7.2.13 Allow unauthorized third parties to access the Division's network and resources.

8. Intellectual Property and IP Rights

8.1 Staff and students shall demonstrate respect for Intellectual Property (IP) rights, and therefore shall:

8.1.1 Demonstrate an understanding that all electronic communication and online content created and related to the Division mandate and function shall be in the custody and control of the organization and be maintained as a component of the corporate record of the organization; and

8.1.2 Learn and use appropriate copyright/citation when prudent to do so.

9. Personally Owned Technology

9.1 Staff and students are permitted to use personal technology at a Division site with respect to the following:

9.1.1 Notwithstanding personally owned accounts (including, data plans, Long Term Evolution (LTE) Networks), a student's connection to the Internet for school purposes shall be to a Division network or partner, and not other (external/neighborhood) networks;

9.1.2 Peer-to-peer (music/video/file-sharing) software or web-hosting services on personal technology that aggressively utilizes the Division's WiFi bandwidth shall not be accessed; and

9.1.3 The security, care, connectivity and maintenance of personally owned technology is the responsibility of the owner; notably:

9.1.3.1 The Division shall not be responsible for the loss, theft or damage of personally owned technology.

9.2 All users will submit a properly signed **Technology Use Agreement Form 640-1** for the use of electronic resources based on the principles outlined above. The acceptable use contract shall include the signature of the user and in the case of a minor, the signature of the parent or guardian. This agreement applies to all situations in which users access information through technology.

Disclaimer: Northern Gateway Public Schools employs a variety of measures to regulate access and information; however, no method is completely effective for enforcing the provisions of this administrative procedure and it

is recognized that there are significant limitations to devices designed to eliminate chance encounter of inappropriate sites.

Reference: Education Act 31, 32, 196, 197, 222 Freedom of Information and Protection of Privacy Act Canadian Charter of Rights and Freedoms Canadian Criminal Code Copyright Act	Date Approved: April 1, 2021 Reviewed or Revised: Executive: January, 2022

References shall be updated as required and do not require additional approval.