Responsible Use of Technology

Purpose

Administrative Procedure 140 (AP) defines the guidelines and expectations for the use of technology within the Grande Yellowhead Public School Division (the "Division"). The purpose of this AP is to:

- **Promote Educational Excellence:** Facilitate the use of technology to enhance communication, collaboration, presentation, and research in support of student learning and achievement.
- **Ensure Responsible Use:** Establish clear expectations for appropriate and ethical technology use by users within the Division.
- **Maintain Digital Security:** Outline procedures to safeguard Division technology and users.
- **Support Digital Citizenship:** Foster a positive and healthy digital culture that emphasizes responsible online behaviour, digital literacy, and cybersecurity awareness.

Authority and Scope

AP 140 applies to all users accessing and utilizing Division technology through Division-authorized or personal devices, including, but not limited to:

- Division-authorized computers, laptops, tablets, and mobile devices
- Division network infrastructure and internet access
- Division email accounts and software applications
- Division-authorized online learning platforms and tools

While recognizing the principles of *Administrative Procedure 105 - Site-Based Decision Making*, the use, procurement, and support of all technology must be coordinated with the Technology Department.

Upon registration each year, every parent or guardian must read, understand, and acknowledge the terms outlined in *Administrative Procedure 140-01 Student Responsible Use of Technology Agreement* regarding their student's use of technology. Any student without an acknowledged *AP 140-01* may be restricted from accessing Division technology resources.

Upon commencing employment with the Division, staff must acknowledge and agree to the terms outlined in *Administrative Procedure 140-02, Staff Responsible Use of Technology Agreement*. Any staff failing to acknowledge *AP 140-02* may be restricted from accessing Division technology resources.

Definitions

Digital Citizenship: the skills needed for individuals to fully participate academically, socially, ethically, politically, and economically in a rapidly evolving digital world.

Division-Managed School Networks (DMSN): includes accessing the internet or Grande Yellowhead Public School Division digital resources while on school property.

Division-Managed Extended Networks (DMEN): includes accessing the internet or Grande Yellowhead Public School Division digital resources during Divisional-operated transportation services.

Multi-Factor Authentication: a digital verification security method which requires multiple forms of identification to access resources and data.

Personally Identifiable Information (PII): any information connected to a specific individual that is used to uncover that individual's identity such as full name, email address, phone number, etc.

Privacy Impact Assessment (PIA): a process used to determine how a program or service could affect the privacy of an individual or organization.

Procurement: the process of sourcing, purchasing, receiving, and inspecting technology goods and services.

Technology: Encompasses all network and device-related items, including, but not limited to:

- Computers (desktops, laptops, Chromebooks, etc.)
- Tablets and mobile devices
- Multi-function devices (printers, copiers, etc.)
- Network infrastructure (servers, routers, switches, etc.)
- Software applications (operating systems, educational software, productivity tools, web platforms, Chrome extensions, etc.)
- Interactive whiteboards and displays
- Audio-visual equipment.

Third-Party Software: any technology such as an application, platform, browser extension, or software that was not created by Grande Yellowhead Public School Division, but are licensed or purchased from external vendors.

Users: refers to students, staff, parents, and other school stakeholders that are using Division or school-based technology.

Procedures

1. **Digital Citizenship**
   - 1.1 All users of Division technology are expected to conduct themselves as responsible digital citizens.
   - 1.2 **Awareness**
     - 1.2.1 Staff complete mandatory Cybersecurity Awareness training modules.
     - 1.2.2 Division email accounts are to be exclusively used for Division-related purposes.
     - 1.2.3 Principals ensure students receive integrated lessons on digital citizenship and digital literacy.
     - 1.2.4 Technology is intentionally utilized to achieve educational objectives.
     - 1.2.5 Users adhere to the privacy policies and terms of use of all utilized technologies.
     - 1.2.6 Users have read and understand the GYPSD Artificial Intelligence Guidelines.

1.3 **Digital Etiquette**

1.3.1 Users engage in appropriate and respectful online interactions.

1.3.2 Users refrain from using Division networks (DMSN or DMEN) or technologies for personal, unrelated GYPSD business, or political purposes.

1.3.3 Staff model and instruct students on digital citizenship best practices.

1.3.4 Staff must supervise students using technology during school hours.

1.3.5 Users take responsibility for online behavior and conduct.

1.3.6 Users immediately report any identified security problems or suspicious activity to the Technology department.

2. **Monitoring and Security**

2.1 **Monitoring**

2.1.1 The Division reserves the right to access, audit, and monitor all digital information without notice or cause.

2.1.2 The Division reserves the right to suspend and/or deny access to technology to maintain system integrity and ensure responsible use.

2.1.3 Video monitoring and recording are conducted per *Administrative Procedure 181: Video Monitoring*.

2.1.4 The Division utilizes web filtering and keyword monitoring to ensure Division safety and block inappropriate content.

a) School administrators are alerted to concerning keywords used by students registered with their school.

2.2 **Security**

2.2.1 Users are responsible for protecting their passwords and maintaining confidentiality.

2.2.2 Passwords must meet complexity requirements and may require periodic changes.

2.2.3 Multi-factor authentication is required for all supported third-party software.

2.2.4 Kindergarten to Grade 3 students may use Clever Badges to access third-party software and Chromebooks.

a) Students requiring accommodations may be permitted to use Clever Badges to access third-party software and Chromebooks.

2.2.5 Only technology authorized by the Director of Information Technology may be connected to Division networks (DMSN and DMEN) or infrastructure.

3. **Accessing and Storing Digital Resources/Data**

3.1 Employment/contract start dates determine access to Division technology unless otherwise authorized by the Superintendent.

3.2 Digital access is terminated immediately upon layoff or departure from the Division unless otherwise authorized by the Superintendent.

3.3 Users ensure that the storage of personally identifiable information (PII) adheres to *AP 180: Freedom of Information and Protection of Privacy* and *AP 185: Records Management*.

3.4 Requests for access to digital resources and data, including PII, must come from the principal or Division department head, unless otherwise authorized by the Superintendent.

3.4.1 User access will be based on job requirements, unless otherwise authorized by the Superintendent.

3.5 Staff are responsible for safeguarding sensitive data and maintaining account and password security.

3.6 Users must secure unattended technologies to prevent unauthorized access.

3.7 Users will only use their assigned credentials in the manner intended. This includes accessing only network (DMSN and DMEN) resources permitted by their login credentials.

4. **Third-Party Software**

4.1 Divisionally accessed platforms and applications are for duties or educational purposes directly related to the Division.

4.2 Staff must review privacy policies, terms of use, and security-related documents before requesting access to third-party software.

4.3 Before use, all third-party software must

4.3.1 Be first approved by the principal or Division department head.
4.3.2 Second and final approval is by the Director of Information Technology.

4.4 *Administrative Procedure 143-03 Privacy Impact Assessments School-Level Checklist* is required for all third-party software collecting Division data.

4.5 Only authorized third-party software will be installed or utilized on Division technology.

4.5.1 Third-party software that requires installation must be done in consultation with the Technology Department.

4.6 Third-party software use must comply with licensing and copyright agreements.

4.7 Users will refer to *AP 143 - Procurement and Maintenance of Technology* for further details on technology acquisition and maintenance.

5. **Liability and Consequences**

5.1 The Division assumes no responsibility or liability for security violations beyond appropriate response to those persons involved in such violations.

5.2 While the Division takes reasonable precautions to restrict access to inappropriate materials on public networks, it assumes no liability for user exposure.

5.3 The Division assumes no responsibility or liability for loss or damage to personal documents stored on Division technology.

5.4 Consequences of inappropriate use of technology may include loss of technology privileges, suspension, expulsion, financial liability for damages, termination of employment, or other actions as outlined in *AP 350 - Student Conduct* or *AP 401 - Staff Code of Conduct*.

6. **Roles and Responsibilities Regarding Technology**

6.1 The following section outlines the roles and responsibilities of the Technology Department and principals or Division department heads regarding technology.

6.1.1 **Technology Department:**

a) Develops a long-range Technology Strategic Plan aligned with the Three-Year Education Plan.

b) Allocates resources for security, administration, support, maintenance, and curriculum integration of technology.

c) Manages the purchasing, upgrading, deployment, and installation of technology.

d) Plans for hardware acquisition, upgrades, reconditioning, software procurement, licensing, and technical upgrades within budget constraints.

e) *Administrative Procedure 143-02 Technologies and Scope of Duties* outlines a further breakdown of technology responsibilities.

7. **Principal or Division department head:**

7.1 Effectively manages and utilizes digital resources to maximize student learning opportunities.

7.2 Ensures appropriate technology integration in curriculum development.

7.3 Provides staff with development for effective technology utilization.

7.4 Coordinates with the Director of Information Technology to authorize appropriate access to technology.

7.5 Ensures implementation of procedures and best practices outlined by the Technology Department.

7.6 Coordinates all school technology procurements with the Director of Information Technology as outlined in *AP 143 - Procurement and Maintenance of Technology*.

8. **Compliance with Related Administrative Procedures**

8.1 Use of Division technology shall be consistent with the following administrative procedures:

8.1.1 Administrative Procedure 143 - Procurement and Maintenance of Technology
8.1.2 Administrative Procedure 145 - Use of Personal Mobile Devices
8.1.3 Administrative Procedure 146 - Responsible Use of Social Media
8.1.4 Administrative Procedure 190 - Use of Copyrighted Materials
8.1.5 Administrative Procedure 181 - Video Monitoring
8.1.6 Administrative Procedure 191 - Copyright and Intellectual Property

9. **Review and Updates**

9.1 This Administrative Procedure will be reviewed and updated as needed to reflect changes in technology, legislation, or Division practices.

Reference: Section 31,32,33,52,53,196,197,222 Education Act
Freedom of Information and Protection of Privacy Act
Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
I.T.I.L. Standards, Alberta Education ATA
Code of Professional Conduct
ISTE Digcit Competencies
Learning and Technology Policy Framework, Alberta Education 2013

Approved: November 2005
Amended: January 13, 2010; September 12, 2016; March 21, 2018; July 1, 2018; April 14, 2020, January 24, 2025