

Administrative Procedure 645

NETWORK AND INFORMATION SECURITY

Background

The Division has, in its possession, confidential information (confidential data) that must be protected. To this end, the Superintendent establishes procedures to ensure the appropriate protection of the Division's information systems.

The Division's various technology systems utilize digital environments and Internet based (Cloud) services and applications as well as cloud storage and electronic file transfer services; as a result, personal information may be stored in electronic format. All personal information is sensitive; therefore, privacy shall be protected during the collection, storage, use, sharing and transmission of all personally identifiable information.

All staff have a statutory and ethical responsibility when using technology and cloud services. Staff shall adhere to the provisions in Alberta's *Freedom of Information and Protection of Privacy Act*, the *Education Act* and relevant Division Administrative Procedures.

Definitions

Cloud Services: shall refer to any Internet or online service or digital information storage provided by organizations or vendors other than Northern Gateway School Division.

Personal Information: as defined in the *Freedom of Information and Protection of Privacy Act*, shall mean recorded information about an identifiable individual, including:

- i) Name, home or business address, or home or business telephone number;
- ii) Race, national or ethnic origin, colour or religious or political beliefs or associations;
- iii) Age, sex, marital status or family status;
- iv) An identifying number, symbol or other particular assigned to the individual;
- v) Fingerprints, other biometric information, blood type, genetic information or inheritable characteristics, and photo likeness;
- vi) Information about the individual's health and health care history, including information about a learning, physical or mental disability;

- vii) Information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
- viii) Another's opinion about the individual; and
- ix) The individual's personal views or opinions, except if they are about someone else.


Portable Storage Device: shall be deemed to refer to any mobile device that can store or process or transmit information digitally. These include, but are not limited to; laptops, tablets, smartphones, thumb/portable drives, CD/DVD.

Procedures

1. With respect to Network Security
 - 1.1 All users of the Division's computer systems and network resources have the responsibility to ensure its overall security and to behave in a manner consistent with this security administrative procedure.
 - 1.1.1. Each user is responsible for understanding and complying with **Administrative Procedure 640 Responsible Use of Technology**.
 - 1.2 The Director of Information Technology shall be responsible for:
 - 1.2.1. Establishing, maintaining, implementing, administering and interpreting network systems security standards, guidelines, and procedures;
 - 1.2.2. Providing specific guidance, direction and authority for network system security;
 - 1.2.3. Providing network backup services;
 - 1.2.4. Establishing and maintaining a network disaster recovery plan; and
 - 1.2.5. Ensuring that Division owned technology has up-to-date antivirus software.
 - 1.3 Staff and/or students shall not:
 - 1.3.1. Establish network services onto any existing Division networks (including, but not limited to: personal web servers, File Transfer Protocol (FTP) servers, news servers, electronic bulletin boards, Really Simple Syndication (RSS) feeds, local area networks, modem connections of any kind); or

- 1.3.2. Make any configuration changes or install any network devices that may have a negative impact on network performance/security.
- 1.4 Any Division owned technology that has been deemed surplus is to be decommissioned and properly disposed of by Technology Services.
- 1.5 Only personnel authorized by the Director of Information Technology or designate shall install applications on servers or workstations.
- 1.6 Each user shall have a unique network account with an encrypted password.
- 1.7 Wireless Networks shall be administered by Technology Services:
 - 1.7.1 Wireless Networks shall have all wireless access points apply the latest security protocols;
 - 1.7.2 Wireless Networks shall utilize the latest encryption protocols;
- 1.8 Personally owned technology shall not be permitted on the internal network, however
 - 1.8.1 A separate wireless Wi-Fi network shall be provided to support personally owned devices.
- 2. With respect to Information Security
 - 2.1 All personal information collected by the Division shall be stored and protected against unauthorized access.
 - 2.2 Portable storage devices shall not be used to store any personal information unless authorized to do so by the Superintendent or designate:
 - 2.2.1 When permitted, the information shall be encrypted and password protected;
 - 2.2.2 Personal information on portable devices shall only be temporary as permitted and removed upon completion of the task.
 - 2.3 Use by staff of cloud-based applications or cloud-based storage shall not include data that contains personal information of staff or students unless:
 - 2.3.1 The privacy agreement with the service provider contains specific clauses compelling them to adhere to the *Freedom of Information and Protection of Privacy Act*;
 - 2.3.2 The service is hosted in a country whose legislation does not have the potential to override the *Freedom of Information and Protection of Privacy Act*;
 - 2.3.3 Any data accessed or transferred must be encrypted and password protected;

- 2.3.4 The Superintendent or designate shall approve all vendor privacy agreements;
 - 2.3.4.1 The agreement is to provide for the security of as well as backup/disaster recovery of data stored.
- 2.4 Division staff shall report any breaches of information security, whether actual or suspected, to their immediate supervisor for investigation.
 - 2.4.1 Supervisors shall contact the Director of Information Technology for assistance with respect to an alleged security breach.
- 2.5 Privacy breaches shall be immediately reported to the Division Head of Privacy (Superintendent) and the FOIPP Coordinator (Secretary–Treasurer) as per **Administrative Procedure 564 Freedom of Information and Privacy Protection**.

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

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