USE OF TECHNOLOGY AND ACCESS TO DIVISION RESOURCES

Background

EICS is committed to protecting the integrity of its learning technology equipment, network, and electronic information. Our district provides access to a secure, equitable computing environment for staff and students while recognizing the need to balance risk and responsible use of technology. Many of the Division provided resources are accessed through the internet using a mixture of Division provided, Division subsidized and Personally Owned Devices (PODs). Use of the Division resources must be in support of education and research and consistent with the mission, beliefs and values of the Division

Examples of these resources are:

- Division provided Internet;
- Division provided access to Email and GSuite for Education;
- Division provided access to internally hosted tools such as PowerSchool, printing, file storage, etc.;
- Access to licensed third party software programs

Resources are not to be used for improper purposes and all laws and existing district policies and procedures apply to conduct while using district information resources. Improper use or behavior includes, but is not limited to the following:

- Creating, displaying, viewing, storing, disseminating or otherwise handling obscene, hateful, pornographic or otherwise illegal materials
- Using the information resources to perpetrate any form of fraud or software, film or music piracy
- Using the information resources to harass others
- Publishing defamatory or knowingly false information about the district, district employees or others on any social media or online publishing site
- Circumventing district security measures
- Undertaking activities which degrade or affect the availability or accessibility of district information resources
- Deliberately introducing malicious software or code into district information resources
- Engaging in any illegal activity using district information resources

Procedures

1 Upon commencement of employment with the district, each employee shall sign a Staff Responsible Use Agreement. Any employee failing to sign the Staff Responsible Use Agreement may be restricted from accessing district information technology resources.

1.1 Accounts for all staff members are granted by the Human Resources department upon receiving the necessary paperwork from the individual.

2 Upon yearly registration every parent and student shall read and agree to the Administrative Procedures identified in the Student Responsible Use Agreement. Any parent or student failing to sign the Student Responsible Use Agreement may be restricted from accessing district information technology resources. Any parent or student failing to sign the Student One-to-One User Agreement will be restricted from using their POD during class time.

3 Any user failing to abide by the terms and conditions of this Administrative Procedure, any associated policies or procedures, or the appropriate Responsible Use Agreement may have their privilege revoked or restricted. As well, users may be subject to disciplinary action.

4 Staff members who fail to abide by the terms and conditions of this Administrative Procedure, any associated policies or procedures, or the Staff Responsible Use Agreement may be subject to disciplinary action, up to and including the termination of employment, as well as the employee may also be subject to legal action. Such disciplinary actions will be consistent with Division policies and procedures and will be in accordance with collectively bargained agreements where appropriate

5 The Division's computer networks and the messages transmitted and documents created on them are the property of the Division. For security and Administrative Purposes, the division reserves the right for authorized personnel to review system use and file content. Any division resources and division provided accounts may be accessed, monitored and audited for compliance without notice.

6 For security and Administrative Purposes, the division reserves the right for authorized personnel to review system use and file content. Any division resources and division provided accounts may be accessed, monitored and audited for compliance without notice.

7 Any use of the system must be in conformity to provincial and federal law, network provider policies and licenses, Board policy and Administrative Procedures. Use of the system for commercial solicitation or political purposes is prohibited. Use of the system for charitable purposes must be approved in advance by the Superintendent or designate.

8 The account owner should not let another individual use their account for any purposes.
- 8.1 Users may not share their passwords with anyone.
- 8.2 Any malicious activity on an account is the account owners' responsibility.
- 8.3 If a user suspects that an account has been compromised, they must report this immediately to the Technology Services Help Desk.
- 8.4 Devices shall not be left unattended when a user is authenticated.
- 8.5 Users should regularly change their passwords every 90 days.

9 Users should familiarize themselves with and utilize safe internet practices such as:
- 9.1 Not clicking on links embedded within unsolicited emails, or emails uncharacteristic of the person who sent them.
- 9.2 Never providing any username or password to websites as a result of an unsolicited email or popup (this is a practice known as Phishing);

9.3 Watching the URL (web address) of the site being visited. A site might “claim” it is the Bank of Montreal, but the actual web address is http://bankofmontral.com (this is an example of a practice known as Spoofing);
9.4 Avoid providing your work email address to unnecessary services or posting it online. Both practices reveal that your email address is legitimate and may lead to an increase in Spam or Phishing attempts.

Shared Credentials

1. All accounts used by more than one person or not directly tied to one person must have a documented responsible employee for communication and management of that account.

2. For any shared or administrative account where the password is known by more than one person, that password must be shared in a secure manner on a need-to-know basis.

   2.1 Only the individual responsible for a shared account may determine who needs to know the password for the account and share the password with those who need it.

   2.2 Individuals using a shared account must strive to maintain the security and integrity of that account.

   2.3 This password must be changed if a person with knowledge of the password is no longer affiliated with EICS.

Device Requirements

The Division reserves the right to restrict or deny the use of devices which do not adhere to the below requirements:

Reference: Section 31, 32, 33, 52, 53, 196, 197, 222 Education Act
Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
Administrative Procedure 143 – Secure Technology Use – Hosted Service or Web 2.0 Tools
Administrative Procedure 146 – Social Media
Administrative Procedure 180 - Freedom of Information and Protection of Privacy
Administrative Procedure 185 - Records Management
Administrative Procedure 350 – Student Code of Conduct
ATA Code of Professional Conduct