USE OF TECHNOLOGY AND ACCESS TO DIVISION RESOURCES

Background

Many of the Division provided resources are accessed through the internet using a mixture of Division provided, Division subsidized and Personally Owned Devices.

Examples of these resources are:

- Division provided Internet;
- Division provided access to Email and Google Apps for Education;
- Division provided access to internally hosted tools such as PowerSchool, Printing, File Storage, etc.;
- Access to licensed third party software programs;

and many more.

These resources are secured using accounts given to each employee of EICS. Properly securing user account access and passwords is a fundamental part of protecting the Division's electronic assets. A weak password or a password that remains for an extended period of time can compromise our entire network and sensitive data.

The intention of this administrative procedure is to have a consistent approach to the secure use of technology that will safeguard personal, institutional, and confidential data for the Division, whether using personal or Division supplied equipment.

This policy applies to all individuals or 'users', regardless of role, capacity, or function who use or access any EICS service, system, network, or computing device. Examples of users include but, are not limited to: staff, students, contractors, visitors, volunteers and organizations granted an EICS account.

Definition

An *account* is defined as a unique identifier (also known as a 'username') used to access EICS electronic resources.

Credentials are comprised of a username and a password associated with the account.

Procedures

Account Provision

1. Account management and assignment are the responsibilities of the Technology Services and the Human Resources departments.

2. Accounts for all staff members, including casuals and substitute teachers are granted by the Human Resources department upon receiving the necessary paperwork from the individual.

3. Before having access to any Division Resources system all users shall sign an agreement to comply with the procedures listed here.

4. The credentials for the account will be communicated directly to the owner of the account.

   4.1 In certain circumstances where direct communication with the owner of the account is not available, the information will be provided to the account owner's direct supervisor.

5. All accounts generated for a full time employee will require a mandatory password change upon first attempt to access a Division networked Windows based computer.

   5.1 Attempts to connect for the first time via any other device, such as iPad, smartphone or personal computer will be denied.

6. Individuals who are not provided with a Division computer (ex: a substitute teacher) will be instructed to change their initial password via a web portal from their personal computer.

   6.1 If this is impossible for any reason, they are welcome to visit the EICS Technology department or the nearest EICS school who will provide temporary and supervised access to a computer for the task of completing their access setup.

Rights and Responsibilities

1. The Division's computer networks and the messages transmitted and documents created on them are the property of the Division.

2. The Division reserves the right to prioritize use and access to the system. The Division reserves the right to remove or disable a user account on the system to prevent further unauthorized activity.

3. 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 is prohibited. Use of the system for charitable purposes must be approved in advance by the Superintendent or designate.

4. The system constitutes public facilities and may not be used for political purposes.

5. 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. Violation of any of the conditions of use may be cause for disciplinary action and 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.

Usage Responsibilities

7. Use of the system to develop or utilize programs in a malicious manner is prohibited. That includes but is not limited to:

   7.1 Installing or using programs which harass other users;

   7.2 Attempting to gain unauthorized access to any computer or computing system or to crack, decrypt or bypass a password securing non-permitted resources;

   7.3 damaging the components of a computer or computing system;

   7.4 any other use of the system which would serve to disrupt the operation of the system by others; system components including hardware, software and infrastructure shall not be destroyed, modified or abused in any way.

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.

9. Use of the Division resources must be in support of education and research and consistent with the mission, beliefs and values of the Division.

10. Users are responsible for the appropriateness and content of material they access, store, transmit or publish using Division resources.

    10.1 Non-appropriate material includes, but is not limited to, hate mail, harassment and discriminatory remarks.

    10.2 Use of the system to access, store or distribute obscene or pornographic material is prohibited.

11. Limited personal use of Division resources is permitted, provided such use

    11.1 Is non-commercial in nature;

    11.2 Is consistent with the degree of professionalism expected from staff members;

    11.3 Does not harm or disrupt the use of the service by others;

    11.4 Otherwise adheres to all aspects of this and other Division Administrative Procedures.

    Examples of acceptable uses could include: the use of computers to access personal email/social media during personal time, the use of the Division email to communicate directly with family members, the reception of a text message from a family member, etc.

Examples of non-acceptable uses include but are not limited to: the use of the Division email to conduct commercial activity not related to the Division, the installation of an app on a phone which consumes large amounts of cellular data paid for by the Division, extended viewing of non-work content on personal devices using the Division provided internet which degrades the internet experience for other users, etc.

12. Computing devices shall not be left unattended when user is authenticated.

13. Users are responsible for familiarizing themselves with and utilizing safe internet practices such as those outlined in the Appendix A.

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:

1. Antivirus

    1.1. Devices used to access Division Resources should be secured by an antivirus program as available on the platform of choice. This includes:

        1.1.1. Laptops and desktops;

        1.1.2. Many cell phones and tablets.

    1.2. Antivirus programs should be configured to remain updated and to automatically scan.

2. Secure Operating System

    2.1. Devices should be kept up to date with security updates as available on the platform of choice.

    2.2. Managed Devices are subject to a number of technical controls established by Technology Services used to establish a minimum level of security on a device. Users of a Managed Device must not attempt to disable or bypass these technical controls without consultation and cooperation from Technology Services.

3. Appropriate use of third party programs

3.1. Devices used to access Division resources might also contain apps or software not purchased or licensed through the Division. It is the responsibility of the user to:

3.1.1. Review the "End User License Agreement and any associated "Privacy Policy";

3.1.2. Verify that the software being installed will not attempt to perform actions which could attempt to disrupt resources for other users;

3.1.3. Verify that the software will not attempt to access or claim ownership of data that could cause a FOIP or security breach.

Appendix B contains a flowchart further outlining general user responsibilities regarding third party programs.

4. Managing Saved Credentials

4.1. Devices which contain saved credentials or which auto-log in to EICS resources must be protected by a password.

4.1.1. For Mobile Devices which are connected to EICS email or other tools, this means they must have an unlock code that is not known to any user other than the EICS employee.

4.1.2. For Personal Computers which auto-login or have saved credentials for EICS email or other tools, this means that the account used to log into the computer must be the sole "Administrator" level account and that those credentials must not be shared with other individuals (including family members).

4.1.3. When using a shared or public device it is important to ensure that credentials are not saved on the device.

Reference: Section 12, 18, 20, 60, 61, 113 School 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
ATA Code of Professional Conduct