ADMINISTRATIVE PROCEDURES

SECTION:	100 – BUSINESS PROCEDURES	**CODE:**	AP 140
PROCEDURE:	**ACCEPTABLE USE FOR ELECTRONIC INFORMATION SYSTEMS**		

BACKGROUND

The Division recognizes the use of electronic information systems as a valuable educational tool and resource. The resources available through this network and the skills that students and staff will develop in using it are of significant value in the educational process. Our goal in providing this service to teachers and students is to promote educational excellence in schools by facilitating resource sharing, innovation and communication.

These opportunities also pose many new challenges including, but not limited to, access for all students, age-level appropriateness of material, access to controversial / inappropriate material, security, rights to privacy, and the cost of maintaining ever more elaborate systems. The Division shall endeavor to ensure that these and other evolving concerns are appropriately addressed, but cannot prevent the possibility that some users may access material that is not consistent with the educational mission, goals and standards of the Division.

The Director or designate shall provide training and procedures that encourage the widest possible access to electronic information systems and networks by students and staff while establishing reasonable controls for the lawful, efficient and appropriate use and management of the system.

All users of Division "Electronic Information Systems" are required to know and abide by the Acceptable Use procedures. These procedures define responsibilities for the safe and acceptable use of the electronic information systems.

PROCEDURES

1. Responsibilities of School Administrators

   1.1 Be responsible for disseminating and enforcing, with help of staff, Division policies and acceptable use guidelines for the Division's electronic information system.

   1.2 Ensure that all student users of the Division's system complete and sign an agreement to abide by Division policies and administrative procedures regarding acceptable use. All such agreements will be maintained on file in the Principal's office.

   1.3 Ensure that all employees using the Division's system complete and sign an agreement to abide by Division policies and administrative procedures regarding acceptable use. All such agreements will be maintained on file in the Principal's office. Principals must make sure that all employees have signed the agreement before access is allowed.

   1.4 Ensure that all students receive training emphasizing the appropriate use of the electronic information system.

1.5 Ensure that all software loaded on computers in the Division is consistent with Division standards and is properly licensed.

2. Access to the System

2.1 All use of the electronic information system must be in support of education and research and consistent with the mission of the Division. The Division reserves the right to prioritize use and access to the system.

2.2 When using the Internet, all students must be under the direct supervision of a staff member.

2.3 Access to the Division's electronic information system will be governed as follows:

2.3.1 Students will be given access to the Division's system only upon receipt of written parental approval.

2.3.2 As appropriate, Division employees will be granted access to the Division's system.

2.3.3 A teacher may apply for a class account and in doing so will be ultimately responsible for use of the account.

2.3.4 Any system user identified as a security risk or as having violated Division and/or school computer use guidelines may be denied access to the Division's system.

3. Access to E-mail and Privacy

3.1 Students may not use any forms of web-based and/or outside email (i.e. HotMail, Outlook, Sasktel, etc.) or chat rooms unless authorized and supervised by their teacher.

3.2 Staff users shall understand that the Division cannot guarantee the privacy or confidentiality of electronic documents. The Division email system is not recommended for personal email messages.

3.3 The Division reserves the right to access e-mail to carry out internal investigations or to disclose messages, dates or files to law enforcement authorities.

3.4 Messages sent as electronic mail are to meet the same standards for distribution as if they were tangible documents or instruments.

3.5 Users are not to open attachments from unknown sources. If an attachment is opened and the computer behaves strangely the Technology Coordinator is to be contacted immediately.

4. Consent Requirements

4.1 No original work, created by any Division student, will be posted on a web page under the Division's control unless written consent has been granted by the student and parent.

4.2 No personally identifiable information about a Division student will be posted on a web page under the Division's control unless the Division has received written consent from the student's parent.

4.3 No personally identifiable information about a Division employee will be posted on a web page under the Division's control unless the Division has received written consent from the staff member.

5. Limited Personal Use - Limited personal use of the system shall be permitted if the use:

5.1 Imposes no tangible cost on the Division;

5.2 Does not unduly burden the Division's computer or network resources;

5.3 Has no effect on an employee's responsibilities; and

5.4 Has no effect on a student's responsibilities.

6. Acceptable Use

6.1 Access to the Division's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of administrative directives and procedures governing use of the system and shall agree in writing to allow monitoring of their use and compliance with such regulations and guidelines. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with Division and school policies.

6.2 Violations of law may result in criminal prosecution as well as disciplinary action by the Division.

7. Prohibited Use

Students and staff are responsible for their actions and activities involving Division computers, networks and Internet services and for their computer files, passwords and accounts. Examples of unacceptable uses that are expressly prohibited include but are not limited to the following:

7.1 Accessing Inappropriate Materials - Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, illegal, promoting violence, or other issues that affect the safety and security of others;

7.2 Accessing Files – Accessing files and/or documents of other users without permission;

7.3 Illegal Activities - Using the Division's computers, networks and Internet services for any illegal activity or action that violates other Division policies, regulations, procedures and/or school rules;

7.4 Violating Copyrights - Copying or downloading copyright materials without the owner's permission (photographs, images, cartoons, logos, digital sound, music files, etc);

7.5 Plagiarism - Representing as one's own work any materials obtained on the Internet (such as essays, reports, articles, etc.). When Internet sources are used in student work, the author, publisher and Web site must be identified;

7.6 Copying Software - Downloading and/or installing unauthorized software or digital media without the express authorization of the Division Technology Coordinator;

7.7 Non-School-Related Uses - Using the Division's computers, networks and Internet services for non-school-related purposes such as private financial gain, commercial, advertising or solicitation purposes or political activity;

7.8 Misuse of Passwords/Unauthorized Access - Sharing passwords, using other users' passwords without permission and/or accessing other users' accounts;

7.9 Malicious Use/Vandalism - Any malicious use, disruption or harm to the Division's computers, networks and Internet services, including but not limited to hacking activities, deleting or modifying system data or software, creating/uploading of computer viruses, and gaining unauthorized access to system passwords in an attempt to obtain Division resources and information; and

7.10 Unauthorized Access to Chat Rooms/News Groups – Accessing chat rooms or news groups without specific authorization from the supervising teacher.

8. Safety of Self and Others

8.1 System users and parents of students with access to the Division's system are to be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material. Users who gain access to such material are expected to discontinue the access as quickly as possible. Students are to immediately report the incident to the supervising teacher.

8.1.1 A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the Division's system and will be subject to disciplinary action.

8.1.2 An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action.

8.2 System users will not reveal personal information about themselves or others, such as: phone number, address, password or username.

8.3 System users will follow appropriate etiquette for both the Division network and the Internet to include but not limited to the following:

8.3.1 Students will not agree to meet with someone they met online, without parent knowledge or participation, while using Division equipment or during school related functions.

8.3.2 Will not use the system to harm the reputation, harass or threaten others.

8.3.3 Will use appropriate language for the educational environment and for the educational activity in which they are currently involved (no swearing, vulgarity, ethnic or racial slurs, or any other inflammatory or threatening language).

8.3.4 Will not transmit (send or receive) obscene pictures or messages.

9. Monitored Use

Electronic mail transmissions, web sites accessed, and other use of the electronic communications system by students and employees are not private and may be monitored at any time by designated Division staff to ensure appropriate use.

10. Web Page Subject Matter

10.1 All subject matter on Web pages is to relate to curriculum, instruction, school-authorized activities, general information that is appropriate and of interest to others, or it is to relate to the Division, or the schools within the Division. All Web site content must be in agreement with the mission, vision, and values of the Division.

10.2 Links from web pages on the Division web server will not lead to commercial web sites that advertise a product or service unless approved by the Director or designate. At no time will such links be for personal gain.

10.3 The Division does not intend to create a forum for free expression purposes. Therefore, neither staff nor students may publish personal home pages as part of the Division web sites, or home pages for other individuals or organizations not directly affiliated with the Division. Staff or student work may be published only as it relates to a class project, course or other school-related activity.

10.4 Each school will identify a web page coordinator for the school. The web page coordinator will be responsible for designing the main site web page and will coordinate the uploading/screening of web pages developed by other personnel. The Principal will act as the final decision-maker for web content.

11. Intellectual Property Rights

11.1 Students shall retain all rights to work they create using the Division's electronic communications system.

11.2 As agents of the Division, employees shall have limited rights to work they create using the Division's electronic communications system. The Division shall retain the right to use any product created for its use by an employee even when the author is no longer an employee of the Division.

12. Security Violations

System users must report any known violations of the Acceptable Use for Electronic Information Systems to a teacher or administrator.

13. Disclaimer of Liability

The Division shall not be liable for users' inappropriate use of electronic information resources, violations of copyright restrictions or other laws, users' mistakes or negligence, or costs incurred by users. The Division shall not be responsible for ensuring the accuracy, age appropriateness or usability of any information found on the Internet.

Reference: Sections 85, 87, 108, 109 Education Act

Date Issued: November 21, 2007