



Acceptable Use of Information Technology

Board Received: June 23, 2008

Review Date: September 2011

Accountability:

1. Frequency of Reports – Annual
2. Severity Threshold – As needed (eg. security threats, interference with normal operations, introduction of new technologies)
3. Criteria for Success – Information Technology resources are used only to enhance the delivery of curriculum and quality of education.
 - Security, safety and productivity of Information Technology resources are maintained.
 - Criminal Code & Board Policy are communicated and followed.
 - Monitoring is performed on an ongoing basis.

Introduction:

The Grand Erie District School Board provides and maintains Information Technology resources and to enhance delivery of curriculum, instructional activities and administration of schools. This Procedure is intended to ensure the safe, secure, ethical and appropriate use of these resources through:

- *education of users regarding what defines Acceptable Use of Grand Erie District School Board Information Technology resources;*
- *enforcement of these definitions.*

Definitions:

In this Procedure:

“Information Technology”, is defined to include but is not limited to:

- personal computers and data devices;
- servers and data storage devices;
- communication networks and associated devices;
- data;
- software;
- systems providing a service that are owned and/or maintained by a third party;
- peripherals

“Communication Networks” is defined to include, but is not limited to:

- GEDSB LAN (Local Area Network)/WAN (Wide Area Network) infrastructure and related equipment;
- LAN infrastructure at a GEDSB user’s place of residence, including a temporary residence;
- Connections to the internet and Internet Service Providers (ISP);

“Peripherals” is defined to include, but is not limited to:

- printers and copiers;
- monitors and projectors ;
- portable data storage devices ;
- input devices

“Users” is defined to include:

- students
- staff
- agencies of GEDSB
- partners of GEDSB
- volunteers
- parents and guardians
- trustees

“Key User” is defined as:

- a staff member within a school, usually (but not necessarily) a teacher, who possesses a degree of advanced Information Technology knowledge, and occasionally performs specific IT-related tasks or functions on behalf of Information Technology Services, and provides some peer-to-peer training and assistance to users.

Roles:

All users: Every user of Information Technology resources at the Grand Erie District School Board has a responsibility to follow this Procedure and take all reasonable measures and to ensure the safe, secure, ethical and appropriate use of Information Technology resources, as outlined herein, at all times.

Additional Roles:

Students: Students should understand that use of GEDSB Information Technology resources is a privilege. They are required to use these resources solely for educational purposes and comply with the directives contained in this Procedure. Students are expected to treat these resources with respect.

Teachers: Teachers are responsible for communicating these expectations to students at least annually. A sample user agreement is attached as Appendix A.

Management: All management will co-operate fully with the school district, local, provincial, or federal officials in any investigation concerning or relating to Information Technology.

Information Technology Services Staff, including Key Users: ITS staff are responsible for providing and maintaining a secure, safe, and productive Information Technology environment, and to enforce this Procedure. This may include, but is not limited to, the activities defined below:

Email: All email and internet communications sent and received by users are the property of the Grand Erie District School Board. Information Technology Services staff will not proactively inspect the contents of a user's email or other personal electronic data unless:

- directed by the user; or
- required by law; or
- required by the Policies of the Grand Erie District School Board; or
- at the direction of Senior Administration in order to investigate complaints regarding email which was intentionally sent or solicited, and is alleged to contain defamatory, inaccurate, abusive, obscene, profane, sexually-oriented, threatening, racially offensive, or illegal material.

Note: School Key Users are strictly limited to the inspection of student accounts only.

Data: Data stored within GEDSB Information Technology resources may be randomly scanned in order to expose instances of unauthorized software and/or data which must be reported to the site's Supervisor and/or deleted.

Unauthorized equipment: Information Technology Services staff are required to disconnect and/or confiscate equipment that is connected to the GEDSB WAN/LAN without prior authorization (i.e. rogue network devices).

Information Technology Services staff may, from time to time, carry out activities which fall under the Unacceptable Activities defined in this Procedure. These activities are to be undertaken by staff ONLY at the direction of Management in order to monitor and enforce this Procedure, and in these specific cases will not be treated as violations.

Information Technology Services staff have privileged access to information and they are expected to report violations of this procedure to their supervisor. In some cases, as required by law, staff may be expected to contact law enforcement agencies.

Information Technology Services staff are strictly forbidden to share or communicate confidential information they come into contact with during their day to day activities. Any violation of this directive will be treated as a violation of this Procedure.

Unacceptable Activities:

The following Unacceptable Activities involving use of the Grand Erie District School Board's Information Technology resources are strictly prohibited:

Unacceptable Content: transmitting, soliciting or willingly accepting, or storing data which contains obscene, indecent, lewd or lascivious material, contains profane language, panders to racism, sexism, other forms of discrimination or other material which explicitly or implicitly refers to sexual conduct. This may include jokes, e-mails, music, videos, sounds or other electronic forms of information.

Hacking: attempting to gain unauthorized access to, or make unauthorized use of, Information Technology resources including, but not restricted to, network security (e.g. accessing websites, downloads or other unauthorized resources) and the introduction of unauthorized software to the Information Technology environment at GEDSB.

Fraud: to obscure the true identity of a user while using Information Technology resources.

Copyright: obtaining and/or storing unauthorized copies of licensed and/or copyrighted material which may include software, music, video, or other such data.

Unlawful Act: violating any laws or participating in the commission or furtherance of any crime or other unlawful act.

Personal Gain: use of the Board's Information Technology resources for unauthorized purposes including, but not limited to, commercial and/or for personal gain, is strictly prohibited.

Personal Privacy: intentionally browsing, copying, deleting, modifying or seeking information about another person's information unless specifically authorized. Access to public information about individuals is deemed acceptable.

Vandalism: intentional defacing and/or damage of Information Technology equipment.

Disrupting Usage: any activity, including the development of automatons, scripts or viruses, designed to disrupt usage of Information Technology resources.

Sharing Confidential Information of Another User: communicating information concerning passwords, identifying codes, personal identification numbers or other confidential information without the permission of its owner or the controlling authority of the school to which it belongs.

Misrepresentation: Users must not share personal security information including passwords, logins, etc, with other users, nor are users allowed to log in to Information Technology resources using an account that has not been specifically assigned to them.

Unauthorized Access: All users are required to have been previously granted authorization to make use of Information Technology resources. This authorization may be granted explicitly to an individual, or implicitly to a group. The failure to prevent unauthorized use of that resource does not relieve an individual of the responsibility of obtaining authorization prior to using the resource.

Enforcement:

ITS staff are responsible for providing and maintaining a secure, safe, and productive Information Technology environment, and to enforce this Procedure.

Activities that are in contradiction of this Procedure will be reported to the appropriate level of supervision or management based on the user involved.

Repercussions may include:

- restrictions on the use of specific Information Technology resources
- suspension of access to all Information Technology resources
- suspension
- expulsion/termination
- criminal charges

Appendix A**Grand Erie District School Board****Student Guide to Acceptable Use of Computers and the Internet****Background**

Computer facilities, which include software, hardware, the internet and other components, are an important ingredient to each student's education at our school.

Each student has the privilege of using these facilities and must use them in an acceptable way.

Acceptable Use

As a general rule, students must use these computer facilities in ways consistent with Provincial and Federal laws as well as consistently with the policies of the School and the School Board.

Unacceptable Use

In order to more fully understand "Acceptable Use", the following outlines activities that are prohibited:

1. Etiquette: transmitting or accepting information which contains swearing, racism or indecent materials. Be polite and respectful.
2. Harm to others: any act harming another individual.
3. Illegal activities: making illegal copies of software (whether licensed or otherwise without the permission of the teacher).
4. Fraud: attempts to deceive others.
5. Vandalism: the deliberate attempt to harm or to disrupt any part of the computer facilities including hardware, software, data or any other component. This includes attempting to harm other installations.
6. Use of the computers for purposes other than education.
7. Personal safety: personal information that identifies the user should not be transmitted over the internet.

School Name	
Student Name	

Code of Behaviour Agreement	
This is to confirm that I have read the Student Guide to Acceptable Use of Computers and the Internet and will abide by the rules and procedures as outlined.	
Signature of Student	Print Name
Signature of Parent	Print Name