ADMINISTRATIVE PROCEDURE	
Approval Date **2017**	*Replacing* **All Previous procedures**
Review Date **2022** **Update September 2017**	*Page* **1 of 9**
Contact Person/Department **Superintendent of Technology Services**	*Identification* **BU-3036**

APPROPRIATE USE OF DIGITAL TECHNOLOGY, CONTENT, AND SERVICES

1.0 PURPOSE

Trillium Lakelands District School Board is committed to providing access to digital technology, digital content, and digital services to enrich educational opportunities for everyone in the school community.

”Digital technology, content, and services include, but are not limited to:

- computers;
- laptops;
- Chromebooks;
- tablet computers (e.g. iPads);
- mobile devices;
- the world wide web;
- learning management systems (LMS);
- digital communication services;
- telephones and telephone system;
- facsimile machines;
- photocopiers/scanners;
- any other personal devices or technologies.

2.0 REFERENCES/RELATED DOCUMENTS

2.1 OP-6020/21 Code of Conduct Policy and Procedure;
2.2 HR-4535/4536 Progressive Discipline Policy and Procedure;
2.3 BD-2030/2031 Freedom of Information Policy and Procedure;
2.4 BD-2120/2121 Privacy Information Management (PIM) Policy and Procedure;
2.5 BD-2035/2036 Records Retention Policy and Procedure;
2.6 BD-2003/2004 Character Development Policy and Procedure;
2.7 BD-2020/2021 Communications Policy and Procedure;
2.8 Personal Information Protection and Electronic Documents Act (PIPEDA);
2.9 Copyright Act;
2.10 Education Act;
2.11 Municipal Freedom of Information and Privacy Act;
2.12 Ontario Human Rights Code;
2.13 Criminal Code.

3.0 TERMS AND DEFINITIONS

3.1 USERS – All employees, students, trustees, parents / volunteers / visitors, members of Board committees, and all other persons given authorized access to Trillium Lakelands District School Board digital technology, content and services.

3.2 DIGITAL COMMUNICATION – E-mail is the Board's standard electronic mail system that allows users to communicate with each other and persons not employed by the Board.

3.3 WIDE AREA NETWORK (WAN) – The WAN is the Board's network between the schools and Board offices including the guest network.

3.4 PERSONAL TECHNOLOGY OR GUEST/BYOD NETWORK – A wireless network that is designed to allow staff, students, and visitors to gain access to a wireless Internet connection with personal devices. This network is secured from the main network to prevent unauthorized access to local network content and resources.

3.5 PRIVACY – The Board is obligated by the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) to carefully manage all "personal information" as defined by the Act and control how it is collected, used, and released. This includes, but is not limited to, not giving out personal information belonging to students, parents, or staff, such as home address, telephone number, age, religion, or family status, without permission. (Note: Not all of the personal information of staff is covered under MFIPPA.)

3.6 SOCIAL MEDIA – Social Media refers to websites that allow users to share content, media, and more. Examples include Facebook, Twitter, and YouTube. All references to any online technology include use of social media.

3.7 CYBER BULLYING - Use of any digital communications, to express comments that are inappropriate and/or profane, disrespectful, slanderous, racist, sexist, libelous, insulting, threatening, hateful, unprofessional, discriminatory, harassing or bullying which are consistent with but not limited to Human Rights, the Board's Bullying and Prevention and Intervention Policy, OP-6215, the Board's Code of Conduct, OP-6020, any applicable professional Standards of Practice, professional advisories, or the Board's Employee Discrimination and Harassment Prevention Procedure HR 4011.

3.8 SOFTWARE/APPLICATIONS (APPS) - The instructions and programming operating inside Computers, Servers, and Mobile Devices to enable them to perform the functions they are designed for.

3.9 CLOUD BASED APPLICATIONS - an application program that functions in the cloud, with some characteristics of a pure desktop app and some characteristics of a pure Web app.

3.10 DIGITAL CONTENT - Any data, files, pictures, or videos stored on or accessed with Computers and Mobile Devices.

3.11 DIGITAL SERVICES - A Network service such as interactive websites, electronic mail, online databases, filing systems, student information systems, business information systems, wikis, blogs, discussion boards, bookmarking and tagging, presentation sites, Digital Content storage, etc.

3.12 BOARD TECHNOLOGY - Includes but is not limited to all Board-provided computing equipment and devices, licensed software and computing services, Internet services used for educational purposes, network hardware, software and bandwidth.

3.13 DIGITAL CITIZENSHIP – The ethical online behaviour of all to respect themselves and others when posting information online.

3.14 INTRANET OR PORTALS - A type of Digital Service provided by the Board to give employees a private and secure online space to work with Digital Content that requires a Network Account and password to gain access.

4.0 ADMINISTRATIVE PROCEDURE

4.1 ACCEPTABLE USE OF DIGITAL TECHNOLOGY, CONTENT AND SERVICES

The use of digital technology, content, and services supplied by the Board is a privilege, not a right and while personal use may be permitted, such personal use does not carry with it any right of privacy or preclude the Board's right to monitor its systems to ensure that this procedure is being complied with. In the course of monitoring its digital technology, content, and services, the Board reserves the right to access and copy files created by users containing personal data stored by the user in the Board's systems – no user has any personal or privacy rights with respect to the Board's digital technology, content, and services or any information stored on the Board's information / communication technology systems.

4.1.1 Relevant federal and provincial laws and regulations apply to the use of the digital technology, content, and services of the Board and all users are expected to comply with these laws and regulations.

4.1.2 Users are expected to use the digital technology, content, and services in a responsible manner consistent with the educational, informational, and recreational purposes for which they are provided. It must be kept in mind at all times that use of the Board's digital technology, content, and services is use of a corporate asset owned by the Board.

4.1.3 Users may access digital technology, content, and services from locations other than their work locations for purposes related to their employment, education, or the furtherance of the Board's business.

4.1.4 All information posted to the Board website / social media; school website / webpages / social media; classroom webpages; and school activity webpages must respect the privacy rights of others, in accordance with MFIPPA;

4.1.5 Use of Trillium Lakelands District School Board's digital technology, content, and services by authorized users may only be used to support the user's education, communication, and research needs, and by staff / others to assist them in the performance of their duties and responsibilities to the Board. All users will adhere to the site and the Board's Code of Conduct and:

a) understand that no user of the Board's digital technology, content, and services has any individual privacy rights in the use of any of the systems or in any information stored in any of the Board's digital technology, content, and services or generated by the use of such systems or services, and, further, be aware that the Board reserves the right to monitor the use of its digital technology, content, and services by any user without notice in order to ensure that the terms of this procedure are being complied with;
b) use digital technology, content, and services in ways that do not disrupt other users or compromise the functionality of the system;
c) observe standards of courtesy and behaviour consistent with the digital citizenship practices and policies of Trillium Lakelands District School Board when sending or publishing messages or other information on the Internet;
d) refrain from using digital technology, content, and services for any purpose which is in violation of the law;
e) use only the login provided to them;
f) maintain password and user ID confidentiality;
g) understand that the Board is not responsible for:
    i) appropriateness of Internet content;
    ii) accuracy or reliability of information located on the Internet;
    iii) loss, damage, or inaccessibility of information due to technical or other difficulties;
    iv) costs or losses incurred by users.
h) understand that saved or deleted digital content, including social media sites, visited on the Internet create a trail of data that may be retrieved at a later date;
i) understand that digital communication sent or received by a user, may be forwarded to other users without the original sender's knowledge;
j) understand that backups of all digital content are made for system recovery only;
k) understand that digital communications and content may not be private;

l) Use a professional tone in all digital communications, and use speech and expression that is appropriate and not profane, disrespectful, slanderous, racist, sexist, libelous, insulting, threatening, hateful, unprofessional, discriminatory, harassing or bullying which are consistent with but not limited to Human Rights, the Board's Bullying and Prevention and Intervention Policy OP-6215, the Board's Code of Conduct OP-6020, any applicable professional Standards of Practice, professional advisories, or the Board's Employee Discrimination and Harassment Prevention Procedure HR 4011.

4.2 UNACCEPTABLE USE OF DIGITAL TECHNOLOGY, CONTENT, AND SERVICES

4.2.1 Users may be subject to disciplinary action for misuse of the digital technology, content, and services. No user should:

a) access the Internet through the Board's digital technology, content, and services for unauthorized, illegal, or unethical purposes;
b) use the Board's digital technology, content, and services to participate in gambling activities, including games of chance and wagering;
c) seek unauthorized access to any of the Board's digital technology, content, and services;
d) seek to damage or alter any of the Board's digital technology, content, and services;
e) knowingly use methods to get around digital technology, content, and services security;
f) send, receive, display, store, or download text, pictures, films, videos or graphics that are illegal, or may reasonably be construed as pornographic, lewd, sexually explicit, defamatory, obscene, or offensive;
g) use abusive, pornographic, lewd, sexually explicit, or defamatory, obscene, or objectionable language in messages;
h) misrepresent oneself or the Board;
i) impersonate other users;
j) lobby elected officials;
k) use digital technology, content, and/or services for personal activities in a way that interferes with the Board's business or the performance by the user of their responsibilities / duties;
l) use the Board's digital technology, content, and services for personal business purposes;
m) knowingly take part in other activities in respect of the Board's digital technology, content, and services that could cause congestion and disruption of the networks and systems;
n) transmit or knowingly receive software or other files which could damage computer systems or software;
o) intentionally delete any digital content, that has informational value, to the detriment of Board operations;

p) attempt to harm, destroy, alter, or copy digital content of any person, digital service or technology without appropriate Board justification;
q) collect, maintain or disclose personal information in contravention of the Municipal Freedom of Information and Protection of Privacy Act; or
r) knowingly transmit or download digital content or software in violation of copyright laws.

4.3 TECHNOLOGY SERVICES DEPARTMENT

The Technology Services Department will:

4.3.1 monitor all information on Board networks; this includes monitoring all files / information stored by users whether related to their personal activities or their activities as students, employees, parents or volunteers of the Board;

4.3.2 make reasonable precautions to limit access to inappropriate materials / information / data;

4.3.3 provide Internet access to schools through the Board's wide area network and guest network;

4.3.4 support schools in taking action when there is inappropriate use of digital technology, content, and services;

4.3.5 ensure that all school websites and webpages are linked to the Board website;

4.3.6 ensure that all classroom webpages and school activity webpages are linked to the school's webpage.

4.4 SUPERINTENDENT OF TECHNOLOGY SERVICES

The Superintendent responsible for Technology Services (TS) will:

4.4.1 when notified by the Senior Manager of Technology Services of any inappropriate content on any Board-supplied technology, determine the appropriate action in consultation with the Senior Manager of Technology Services and other senior management as necessary on a case-by-case basis;

4.4.2 review and revise wording on the student registration form as needed.

4.5 SENIOR MANAGER OF TECHNOLOGY SERVICES

The Senior Manager of Technology Services will:

4.5.1 notify the Superintendent Responsible for Technology Services of:

a) any inappropriate content on any Board-supplied technology;
b) any technology misuse – including misuse of hardware, software, and security / virus tools.

4.6 TECHNOLOGY SERVICES STAFF

Technology Services staff will:

4.6.1 provide technical support for Board technology only – this includes hardware, software, and security / virus management tools.

4.6.2 report any technology misuse to the Senior Manager of Technology Services – this includes any misuse of hardware, software, and security / virus tools.

4.6.3 offer training for staff on the use of the Internet, digital citizenship, and provide resources to help staff train students on appropriate use of digital technology, content, and services as required or requested.

4.7 SUPERINTENDENTS, PRINCIPALS, AND SUPERVISORS

Superintendents, Principals, and Supervisors will:

4.7.1 ensure information / communication technology protocols are communicated to new staff upon hiring;

4.7.2 ensure all classroom webpages, and school activity webpages are linked to the school's webpage;

4.7.3 ensure they are aware of all digital communication methods used by all teachers;

4.7.4 not accept any donated technology without permission of the Senior Manager of Technology Services as this may negatively impact on the Board's ability to effectively license, manage, secure and support solutions for classroom programs;

4.7.5 apply appropriate measures to address any staff or student user violations of information / communication technology digital technology, content, and services protocols.

4.8 PRINCIPALS AND SUPERVISORS

Principals and supervisors will:

4.8.1 coordinate and manage digital technology, content, and services facilities and resources in the school for staff and students;

4.8.2 ensure staff and students adhere to the acceptable use of personal technology when used in any Board facility as per 4.2.1 m) above;

4.8.3 report student abuse of digital technology, content, and/or services to the Senior Manager of Technology Services;

4.8.4 report staff abuse of digital technology, content, and/or services to the Superintendent of Technology Services;

4.8.5 when deemed appropriate, take disciplinary steps when inappropriate use of digital technology, content, and/or services occurs:

a) students – take action as appropriate in the Student Code of Conduct Policy and Procedure;
b) staff – contact the appropriate Area Superintendent of Learning and Superintendent of Employee Services department and take action as appropriate in the Progressive Discipline Policy and Procedure.

4.9 STAFF MEMBERS

4.9.1 All staff will:

a) take reasonable precautions to ensure the security of equipment and information storage when transporting Board technology;
b) ensure assigned technologies are password protected and encrypted. Materials containing the personal information of students or staff must be protected as outlined in the operating procedures of each department;
c) ensure that all devices that receive forwarded Board digital communication are password protected;
d) ensure that all information contained on portable storage media, which is confidential, and not limited to staff information, student information, and/or student marks are password protected.

4.9.2 In addition to 4.9.1, school staff will:

a) as part of the student registration process, maintain records of signed parent consent;
b) take reasonable steps to supervise the use of the Internet;
c) instruct users on the appropriate use of technology and the Internet;
d) require that any school information posted to school webpages comply with the Freedom of Information and the Protection of Privacy Act;
e) inform students that activities and files are subject to inspection by school and Board staff; and
f) report to their principal any inappropriate content on any Board-supplied technology of which they become aware.

4.9.3 In addition to 4.9.1 and 4.9.2, teachers will:

a) manage and actively supervise student use of digital technology, content, and services in their assigned teaching areas and when acting in a supervisory capacity;
b) ensure that all students have permissions reviewed and signed on registration forms regarding appropriate use of digital technology, content, and services.

4.10 USE OF PERSONAL TECHNOLOGY (BRING YOUR OWN DEVICE - BYOD)

Users who choose to bring personal communication and/or computing devices to school do so with the understanding that:

a) Personal communication and computing devices that are brought to school are the responsibility of the owner. The Board and/or the school are not liable for damage, loss or theft of the device or data that is stored on the device.
b) Personal communication and computing devices may not be used at any time where individual privacy must be protected such as washrooms, locker or change rooms.
c) When using personal devices both on and off the Board network to access the Board's digital content or services, users are subject to the appropriate use of technology policy and/or the Code of Conduct.