Effective: February 10, 2020

SUPERIOR NORTH CATHOLIC DSB

Administrative Procedure: Acceptable Use of Technology for Users

Table of Contents

1.0 Terms and Definitions

1.1 **Social Media refers** to websites and applications that enable users to create and share content or to participate in social networking.

1.2 **Information Technology** refers to all forms of technology used to create, store, exchange, and use information in its various forms (data, audio, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived).

1.3 **E-communication, or electronic communication**, refers to the transfer of writing, signals, data, sounds, images, signs or intelligence sent via an electronic device.

1.4 An **employee** is a person who performs any work for, or supplies any services to an employer for wages.

2.0 Guidelines

2.1 The Board offers the guidelines listed below for Users who use online social networking applications that may be frequented by employees. The Board also reserves the right to monitor social media use.

2.2 **Model appropriate behaviour**: As a digital citizen, model the behaviour that you expect to see online from students. Alert students to appropriate online behaviour and the proper use of comments and images.

2.3 **Privacy settings and content**: Set and maintain strict privacy settings by choosing settings that limit what others can do and see. Avoid blanket invitations that use your email contacts automatically. Exercise care with your profile content by posting thoughtfully and reviewing periodically for appropriateness. You should always consider your privacy settings before sharing information.

2.4 **Friending students**: Users must decline student-initiated requests and never initiate a friend request with a student. Users should not follow students on Twitter. Users should not exchange private texts, phone numbers, personal email addresses or photos of a personal nature with students.

2.5 **Maintain a professional persona**: Communicate with students electronically at appropriate times of the day (8:00 a.m. - 4:00 p.m.), through Board established and approved platforms, and about school related content. Use a formal, courteous and professional tone in all communications to ensure that professional boundaries with students are maintained.

2.6 **Other friends**: Remind all other members of your network of your position with the Board and monitor their posts to your network accordingly. Also, be mindful in your postings to all friends' sites, and act immediately to remove from your site any material that may be inappropriate, whether posted by you or someone else.

2.7 **Groups in your social network**: To remain consistent with the values of our Board, associate with social networking groups that reflect a diverse educational environment in which both students and adults practice tolerance and accept competing views.

2.8 **Course use of social networking**: If you are a teacher, advise the school principal when using social networking tools for teaching. The same care must be taken in choosing such tools as other course resources and materials.

2.9 **Be transparent and authentic**: Use your true professional identity at all times. Users who use social networks for Board purposes must do so using their own.

2.10 **Public information**: Recognize that many former students have online connections with current students, and that information shared between Users and former students is likely to be seen by current students as well.

2.11 **Be respectful and responsible**: Avoid online criticism about students, colleagues, parents/guardians, the Board, other Users, or others within the Board community. Avoid impulsive, inappropriate, demeaning or heated comments.

2.12 **Privacy and confidentiality**: Respect the privacy and confidentiality of information pertaining to students, parents/guardians, other Users, and other members of the Board community. This includes student or User information, photographs or videos of students or Users, financial information, Board plans, marketing information and Board development information.

2.13 **The Board's Acceptable Use of Technology Policy**: Ensure that you are aware of and comply with the Board's policies and procedures regarding the use of social media/e-communication and the appropriate use of electronic equipment.

3.0 Access and Use

3.1 The use of technology is intended for Superior North Catholic District School Board (the "Board') purposes. The term "technology" in this policy refers to computers/tablets, cell phones, database/record systems, networks, software, email systems, voicemail, fax transmission and use of and access to the intranet and internet. Users (as such term is defined in the Acceptable Use of Technology (Users) policy, the "Policy") may make limited personal use of Board technology provided that Users do not compromise their obligations to the Board and they comply at all times with the terms of the Policy, this Administrative Regulation, and other Board policies and Board guidelines as applicable. Each User shall use the technology in a fashion consistent with the Board's values, and in an ethical and lawful manner.

3.2 The use of Board Network is accessed through Board provided devices. Usage of personal devices are not permitted to be connected to the Board's Network. The Board will provide a Guest network for such usage.

3.3 Pictures, audio and visual recordings of students must remain on Board's appointed devices. Staff are not permitted to use their own personal devices for such activities.

3.4 Examples of conduct that violate the Policy are as follows:

3.4.1 using Board technology to create, process, distribute or access illegal, offensive, pornographic and/or inappropriate materials;

3.4.2 sending defamatory, abusive, obscene, profane, sexually oriented, threatening or racially offensive messages;

3.4.3 failing to immediately remove any defamatory, abusive, obscene, profane sexually oriented, threatening or racially offensive messages that are received;

3.4.4 downloading, storing or sharing illegal, inappropriate, offensive or obscene material on Board-owned computer systems;

3.4.5 downloading, storing or sharing on Board-owned computer systems media files, including music and video files that are illegal, offensive, obscene, inappropriate or that infringe on copyright, including music and videos;

3.4.6 knowingly accessing sites containing sexually explicit, racist, homophobic or other material clearly inappropriate in a Board environment;

3.4.7 uses that are malicious, unethical or in violation of accepted community standards and/or Board policies;

3.4.8 uses that violate any federal or provincial laws, including the Ontario Human Rights Code;

3.4.9 using your Board email address for non-work related purposes;

3.4.10 knowingly creating, exchanging, transmitting and/or downloading messages or data that are offensive, harassing, obscene, libelous, abusive, discriminatory, or threatening or that encourage violence;

3.4.11 conducting activities which are unrelated to the User's duties and responsibilities to the Board during business hours;

3.4.12 advertising or soliciting, including advertising of personal services;

3.4.13 attempting to access another person's account or private files or misrepresenting yourself as another person in electronic communications;

3.4.14 not using electronic hand-held devices while driving on Board time and business;

3.4.15 sending anonymous or inappropriate unsolicited email messages, including mass email messages, such as chain letters, jokes or spam through Board email;

3.4.16 computer-hacking and related activities; and/or

3.4.17 attempting to disable or compromise the security of information contained on Board computer systems.

3.4.18 Use of personal devices to record voice/videos or take images of students or their work.

3.5 All Users will ensure that all communication is in compliance with applicable privacy legislation, and that all records in the custody and control of the Board that contain personal information that pertains to a student, User or other individual will be maintained in strict confidence.

4.0 Content

4.1 Each User is responsible for the content of all text, audio or images that he or she accesses or sends via the internet and phone systems, and for ensuring that the communications and messages conform in all respects to the Policy and the Board's mission, vision and values.

4.2 Each User needs to exercise caution to prevent virus and spyware contamination. If any User detects such contamination, the User must report it to Board information technology staff immediately.

5.0 Passwords and Information Security

5.1 The use of passwords is intended to ensure that only authorized individuals have access to the Board's technology and the private and confidential information it contains. Users shall not disclose passwords issued to them to any other person. Users shall not disclose passwords or use passwords provided to them to permit other persons to access the Board's technology. Each User shall be responsible for all activities arising from the use of his or her password.

5.2 Each User shall take reasonable precautions to protect the integrity of the Board’s systems and to prevent unauthorized access to the technology. For example, Users, before leaving computers unattended, will use a password protected screen saver, and/or log off.

6.0 Privacy

6.1 Each User has a reasonable expectation of privacy with regard to use of voicemail and email, and digital information that is stored on its computers.

6.2 If and/or when the Board has reason to believe that there has been a violation of this policy or procedure, then the Board has the right, but not the obligation, to inspect any computer or computer systems, and to monitor the use of any of the technology, including, without limitation, inspecting the contents of voicemail and email messages. Users will be notified when such monitoring is to take place, and whether monitoring has occurred. In certain situations, the Board may be compelled to access, read, copy, reproduce, print, retain, move, store, destroy and/or disclose messages, files or documents stored in or sent over its email, internet or computer systems. These situations may include the following:

6.2.1 in the course of regular maintenance of the computer system;

6.2.2 in the event of a request for documents as part of litigation or similar proceedings; or

6.2.3 where the Board has reason to believe that the computer system is being used in violation of the Policy.

6.3 Unauthorized access by any User of another individual’s electronic information is a violation of the Policy. Access by a User of another individual’s electronic information will only be permitted with the written approval of the Superintendent responsible for the information technology department or his or her delegate. IT personnel must sign for the appropriate reasons they need to access someone’s computer.

6.4 There is a distinction between the professional and private life of a User. Users are individuals with private lives; however, off-duty conduct matters. Sound judgment and due care needs to be exercised. Users must maintain a sense of professionalism at all times in their personal and professional lives. Activities that are improper, unethical, illegal, or that cause undue discomfort for students, parents, other Users, or other members of the Board community should be avoided in both physical space and cyberspace.

7.0 Social Network and E-Communication

7.1 Examples of social networks include (but are not limited to) Facebook, Twitter, LinkedIn, Flickr, YouTube, Wikipedia, Snapchat, WhatsApp, Instagram, etc.

7.2 Some examples of e-communication are email, text messages, social media messaging and image sharing.

7.3 Social networks are becoming increasingly popular with people of all ages and in some cases have become virtual meeting places for Users, students and others. It is important to know that Canadian courts hold educators to a higher standard of conduct and behaviour than the general public, even when an educator is not officially representing his or her Board.

7.4 Social networks and electronic communication can be effective when used cautiously and professionally. They serve a range of purposes, from helping students and parents/guardians access assignments and resources related to classroom studies, to connect with classrooms in other communities and countries.

7.5 While Facebook pages (or groups) and other social media established solely for classroom use are allowed to facilitate learning, each User must at all times use such tools in ways that are consistent with the mission, vision, and values of the Board and in ways that comply with the Ontario College of Teachers' advisory on the use of social media. Users must also inform their principal if they are using social media in their classroom.

7.6 Users also use the internet and social networking sites as instructional tools, for professional development, and to seek information on lesson plans, new developments and methodologies.

7.7 Each User is governed by the Policy in all online spaces and is expected to conduct him or herself respectfully and responsibly. It is the responsibility of each User to know and respect proper professional boundaries with students, even when students initiate electronic interaction.

7.8 There may be occasions when Users come across each other's social networks. Should there be concern regarding appropriate behaviour, it is ideal to address the concern directly with the person involved. If for a particular reason a User is uncomfortable doing so, another option is to contact the school principal or supervisor.

8.0 Support

8.1 The Board's information technology department is not in a position to support hardware or software other than that of the Board.

9.0 Violations

9.1 Users are expected to maintain the Board's values and the integrity of its technology. For this reason, any User found to be abusing the privilege of the Board regarding use or access to its technology or contravening the terms of the Policy will be subject to disciplinary action, up to and including possible termination of employment. The Board also reserves the right to inform appropriate law enforcement authorities or other officials of any offences or possible offences under the Criminal Code or other applicable statutes.

9.2 Users are expected to return equipment in the condition given to them originally. They should not affix any items (ie. name stickers) to the equipment and should not eat or drink near it. Consequences for not caring for equipment will be payment or replacement by the User.

9.3 If any User needs clarification regarding the appropriate use of the Board's technology, they are encouraged to direct their questions or concerns to the Director of Education or designate.

9.4 Please keep a copy of the Policy and this Administrative Procedure for your reference.