Responsible Use of Technology

Date: 2013 04 23 / 2022 04 19

Administrative Procedures

1. Responsibilities

1.1 The Treasurer of the Board will be responsible for the implementation of this policy and procedures and ensuring compliance.

1.2 The Manager - Information Technology Services will:

1.2.1 Ensure awareness exists throughout the board.

1.2.2 Obtain approval of proposed amendments to the procedure and ensure communication of such amendments.

1.2.3 Communicate the purpose and contents of the procedure.

1.2.4 Administrate the procedure, including regular reviews of content, ensuring all users have access to cybersecurity training materials.

1.3 All Staff Supervisors will:

1.3.1 Be responsible and accountable for ensuring all individuals under their accountability are aware of this policy and procedures.

1.3.2 Be responsible for contacting their supervisor or the help desk to request advice concerning this policy and procedure.

1.3.3 Be responsible for reporting non-compliance with this policy or procedure or suspected policy and procedure violation cases to their supervisor, human resources, or Information Technology Services.

1.4 All Users will:

1.4.1 Be responsible Catholic digital citizens by being familiar with and complying with this policy and procedure.

1.4.2 Be responsible for being familiar with the Board and School Code of Conduct.

2. Expectations

Access and Access Control

2.1 Users must only request system access to information or assets required to perform their job responsibilities.

2.2 Supervisors must review and approve appropriate access for staff to efficiently fulfill their job responsibilities. Staff member changes due to role transfer, retirement or career change, the supervisor leader must ensure access rights are adjusted accordingly.

2.3 Administrative staff and school office using any electronic means must do so using board-approved devices.

2.4 Bring Your Own Device for students and teaching staff will only be granted access to the Board systems after signing the BYOD Agreement. Third-party requests for access must contact the help desk through their board contact.

2.5 Users are responsible and accountable for all actions performed with their User accounts.

2.6 Upon request, leave of absence, or termination of employment, Board technology must be returned to human resources, supervisor, classroom teacher, principal or Information Technology Services.

2.7 Staff must use assigned administrative or high-privilege accounts only when performing duties requiring this type of access. In all other cases, users must use their general role-based non-privileged account.

2.8 Users must be responsible for adequately protecting and securing Board information in all media and locations. They must not attempt to circumvent access control or other security mechanisms.

2.9 Users must not leave Board devices unattended without enabling a password-protected locked screen.

2.10 Users of Board mobile devices will reimburse the Board for personal use not related to Board business.

2.11 Incidental personal use of the Internet (e.g., banking, news) is permitted provided it does not impact productivity. Personal use of information on the Board's technology is at the user's own risk.

2.12 Users should be aware that the Board has the right to monitor, record, and archive all emails and other electronic communications received, stored, and reproduced using Board Technology or a personal BYOD device. Users should not have any expectation of privacy.

Safeguard and Protect

2.13 Users must ensure that all Board passwords are kept confidential and use multi-factor authentication whenever possible. If you suspect your access has been compromised, you must immediately change passwords and notify the help desk.

2.14 Users must not share passwords or PINs, including sharing with family or other household members. Users must not communicate passwords in a readable format, including writing them down on paper and sending them to others electronically.

2.15 Users must not re-use their Board passwords for personal account access, personal e-mail, or banking.

2.16 Users of Board technology are expected to take reasonable measures to secure the devices. Ensure laptops are not left unsecured in plain view.

2.17 Communication of confidential board records must be completed on Board-approved email, and devices for creation, transmission, storing, processing or otherwise.

2.18 Communication using tools such as e-mail, chat, text, must be used in a responsible, respectful and lawful manner, which must be in compliance with the Board Mission Statement; Code of Conduct; and Anti-Spam Laws, CASL.

2.19 Users must not open email attachments from unknown sources or click on links to unfamiliar websites. Suspicious emails must be reported using the phishing reporting feature in the email system. If in doubt, report activity to the help desk.

2.20 Information Technology Services will conduct periodic Phishing tests.

2.21 Users are not authorized to download or install software onto Board technology. Software must be approved by Information Technology Services to meet licensing, copyright, and privacy requirements.

2.22 Staff must follow the "vetting new software process" to meet our procurement policy and procedures.

2.23 Users when there is reasonable cause to suspect inappropriate conduct or illegal acts using the Board's technology, an investigation will occur upon appropriate consent or where ordered to do so by law. Consent requires two of the following: Director of Education, Treasurer of the Board, or Chair of the Board.

2.24 Violation of the Responsible Use of Technology policy and procedures may result in restricted network access, liability for the cost of remediation, disciplinary action up to and including dismissal in matters concerning staff; and disciplinary action up to and including suspension and expulsion for issues concerning students. Legal action including, but not limited to, criminal prosecution under appropriate provincial and federal laws may also be initiated.

Definitions

Board Technology – any Board owned computers, servers, network, software systems and applications, mobile devices, data storage, personal devices that are used to access information technology.

Bullying – aggressive and typically repeated behaviour that causes harm, fear or distress to another individual including physical, psychological, social or academic harm to the individual's reputation or property.

BYOD – stands for bring your own device, which is a personal device.

CASL – Canada's Anti-Spam Legislation. Generally, the legislation prohibits the sending of commercial electronic messages unless prior consent of the recipient is obtained and the sender's identity information and unsubscribe mechanism is included in the commercial electronic messages. The legislation also prohibits the altering of transmission data, email harvesting and the installation of computer software without express consent.

Cyber-bullying – includes bullying by electronic means.

Devices – References to electronic equipment include current and emerging technologies capable of recording, storing, processing, communicating, and transmitting information, images or sound digital.

High-Privileged Account – a type of account that has additional authority to modify system-wide settings or has access to privileged information.

Mobile Devices – All cellular, or internet-connected mobile Technology devices, including smartphones and tablet devices, whether Board owned or Personal Devices.

Multi-Factor Authentication - authentication method that requires the user to provide two or more verification methods to gain access to the network or resource such as an application.

Network - The Board's technology infrastructure includes all related Board-managed systems.

Non-Privileged Account – a type of account that does not have authority to see privileged information or modify system-wide settings.

Personal Devices – All non-Board owned devices.

Personal Information (MFIPPA: s 2.1) - Recorded information about an identifiable individual, including:

a) Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
b) Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
c) Any identifying number, symbol or other particular assigned to the individual,
d) The address, telephone number, fingerprints or blood type of the individual,
e) The personal opinions or view of the individual except if they relate to another individual,
f) Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
g) The views or opinions of another individual about the individual, and
h) The individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Phishing – A technique used by criminals to gain personal information using fraudulent emails that

appear to come from legitimate entities and companies.

PIN – Personal Identification Number is a numeric passcode used in the process of authenticating a user to accessing a system.

Record – is an Electronic Record, "any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system." This definition ensures that electronic records are the same as paper records. For example, student record, staff record and may contain recorded information about an identifiable individual.

Spam – Unauthorized and/or unsolicited electronic mass mailing.

Staff – includes all paid employees of the school or the Board.

Staff Supervisors - includes principals, teachers, supervisors, superintendents, managers and other employees that lead employees and students of the school or the Board.

User - Includes trustees, administrators, academic and support staff, students and parents, visitors, volunteers, and persons associated in any way with the Board.

Applicable References

Legislation

- Bullying Prevention and Intervention (PPM 144)
- Canada's Anti-Spam Legislation (CASL)
- Education Act, Ontario: s266; s171(38)
- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA): MFIPPA
- Provincial Code of Conduct (PPM 128)
- Ontario College of Teachers, Professional Advisory: Use of Electronic Communications and Social Media (2017)

Appendix A: Unacceptable Use

All users shall use technology in a manner consistent with the Board's values, code of conduct and in an ethical and lawful manner Examples of conduct that violate the policy are as follows:

a. Knowingly, accessing, copying, downloading, storing, or transmitting material, including music and video, that contains or could be considered defamatory, racist, sexually explicit, homophobic, threatening, and/or inappropriate materials that clearly inappropriate in school or work environment that may offend or degrade others.
b. Transmit any files, information or materials designed to disrupt or tamper with data or networks maintained by the Board or any other person. Such as scanning network, installing malicious programs virus, worms, trojan horses and email bombs.
c. Sending or forwarding anonymous or inappropriate unsolicited email messages, including mass email messages, such as chain letters, jokes, or spam
d. Must not give out personal information, whether of the user's or of any other person.
e. Attempting to access another person's account or private files or misrepresenting oneself as another person in electronic communications.
f. Must not include any inappropriate information or confidential information in email communication whether of the user's or of any other person.
g. Downloading, installing, or sharing unauthorized or improperly licensed software.
h. Uses that violate any federal or provincial laws such as using technology to record without consent.
i. Conducting business activities which are unrelated to the user's duties and responsibilities to the Board.
j. Advertising or soliciting, including advertising of personal services.
k. Cyber-bullying, creating a web page or a blog in which the creator assumes the identity of another person.
l. Cyber-bullying, by impersonating another person as the author of content or messages posted on the intranet/internet.
m. Cyber- bullying, communicating material electronically to more than one individual or posting material on a website that may be accessed by one or more individuals.
n. Teaching staff have the right to determine how and when technology will be used by students during instructional periods, regardless of the ownership of the device.