Staff Acceptable Use of Technology

1.0 Purpose

To establish clear expectations for the responsible, safe, and appropriate use of Fusion Collegiate's network and information technology (IT) resources by staff, contractors, and volunteers.

2.0 Background

Fusion Collegiate provides access to IT resources to support teaching, learning, and business operations. All users are required to comply with this administrative procedure when accessing Board-owned IT resources or when using personal electronic devices for educational or business purposes.

Fusion Collegiate reserves the right to access, audit, and monitor all Board-supplied IT resources, without prior notice, to ensure system integrity, security, and responsible use. Violations of this procedure will be addressed in accordance with related Board administrative procedures.

3.0 Authority and Responsibility

3.1 The Superintendent is responsible for the administration and implementation of this administrative procedure.

3.2 Administration and IT staff are responsible for managing access, security, and monitoring of IT systems.

4.0 Network Access

4.1 Network access is provided for the following purposes only:

a) Educational use to support teaching and learning,

b) Business use for communication and marketing,

c) Limited personal communication, provided professional responsibilities are not compromised.

5.0 Responsible Use of Technology

5.1 Staff, contractors, and volunteers shall:

a) Comply with all Board administrative procedures related to technology use,

b) Use IT resources in a respectful, responsible, and lawful manner,

c) Be accountable for all actions performed while logged into Board systems,

d) Use appropriate language and images in all digital communications,

e) Comply with copyright legislation and proper citation requirements,

f) Use only assigned user accounts unless authorized by administration or IT,

g) Use IT equipment, bandwidth, and storage responsibly,

h) Maintain the confidentiality and security of passwords,

i) Log off workstations when unattended and at the end of the workday,

j) Not attempt to bypass, disable, or modify network security measures,

6.0 Password and Account Security

6.1 Staff members must enable two-factor authentication on all devices (corporate or personal) that access Fusion information and data.

6.2 Device passwords shall:

a) Meet System Account Administrator requirements,

b) Remain confidential and secure,

c) Not be written down, shared, emailed, or embedded in automated login processes.

6.3 Users shall ensure systems are not left in an unsecured state and shall log off when leaving a workstation for any length of time.

7.0 Safe Use

7.1 Staff, contractors, and volunteers shall:

a) Protect personal and confidential information,

b) Report inappropriate material, security concerns, or network issues to administration or IT,

c) Understand that web filtering is used but may not block all inappropriate content,

d) Not distribute inappropriate or prohibited content,

e) Staff must ensure that any use of Generative AI tools complies with student privacy standards and does not involve the upload of personal information.

8.0 Appropriate Use

8.1 Staff, contractors, and volunteers shall:

a) Obtain consent before photographing, recording, publishing, or sharing personal information or images,

b) Obtain permission when sharing jointly created electronic data,

c) Use IT resources in a manner that does not disrupt system performance or compromise security,

d) Not use Board IT resources for political lobbying, advertising, personal profit, or private business,

e) Download, save, or install software and media only in accordance with acceptable use standards and copyright laws,

f) Not destroy records subject to a request under the POPA and ATIA,

g) Safeguard sensitive and confidential information and seek guidance when required,

h) Staff shall maintain professional boundaries on all digital platforms:

- avoid private electronic communication with students through non-Board sanctioned channels (e.g. personal DMs) – 3CX is available.
- avoid public communication regarding school-based activities and operations on social media

9.0 Personally Owned Devices

9.1 Staff, contractors, and volunteers using personal electronic devices shall:

a) Access the Fusion Collegiate Guest Network only (not the Staff network),

b) Sensitive files and student records must be stored within FEA-approved cloud environments and not saved to the local storage of personal devices,

- All Fusion data is through our corporate Microsoft Account only.

c) Acknowledge that activity may be monitored and traced to the user,

d) Connect only to the wireless network,

e) Maintain current virus protection where supported,

f) Disable peer-to-peer sharing and hosting services while connected,

g) Use devices appropriately during instructional or work time,

h) Assume responsibility for the security, maintenance, and support of personal devices,

i) Understand that Fusion Collegiate is not responsible for loss, theft, or damage to personal devices.

Legal References

Protection of Privacy Act (POPA), Access to Information Act (ATIA), Canadian Copyright Act

Approval and Review

Revised: February 2026