#113588

IJNDC, IJNDC-E-1, 2
GBEF
JICFB
JK

Acceptable Student Use of Digital Technologies and Electronic Communication

Student use of School Division networks and technology is intended for educational purposes only and is to be considered is a privilege, not a right. This regulation is provided to make all students aware of the responsibilities associated with respectful, ethical, and lawful use of Division technologies and resources.

Internet use is an important component of the integration of technology and communications with learning in the School Division. Teachers will guide students to become responsible digital citizens in order to:

- access information on topics studied in the classroom
- communicate rapidly with other users around the world
- collaborate with others in different locations on topics of common interest
- become competent global citizens with a strong 21st century skillset.

A. <u>General Student Responsibilities</u>

While using technology at school, it is expected that students shall:

- accept ultimate responsibility for their actions in accessing technology
- access the network and the Internet only under the supervision of instructional staff and accept any limitations or restriction placed on them by the Division IT Department
- abide by all applicable copyright and intellectual property laws
- close all Internet browser windows and log off the Divisional network when not directly using the computer or mobile device
- use good judgment at all times
- follow generally accepted network etiquette rules, including using appropriate language and content in all correspondence or communications
- treat others with respect and not harass another person or engage in inappropriate behaviours as per policy JICFB Student Harassment and Bullying and JK Student Conduct
- respect the rights and privacy of other technology users
- use only the Divisional accounts (e.g. network login, e-mail) assigned to them by the IT Department; and keep all user IDs and passwords for Divisional accounts confidential
- not independently attempt to modify settings, install software or uninstall software previously installed by the Division IT Department
- access only Internet sites with content appropriate for a school environment
- use only Division managed or endorsed technology and communication systems unless otherwise approved under the guidelines and procedures of the Division's Social Media Policy

- refrain from revealing personal information about themselves and others online, which includes, but is not limited, to the student's name, age and location
- connect personal devices only to the secure wireless network in the interests of protecting the integrity and reliability of the Division's corporate network
- respect the direction of their teachers as to when, and what technology use is appropriate while in class
- understand the consequences of inappropriate use of technology, as outlined in this policy

The following list details some examples of prohibited activities based on student responsibilities outlined above:

- Any action that violates existing Division policy, public or copyright law
- Accessing another's personal accounts or passwords without permission
- Disclosing any passwords to another user or to a third party
- Releasing personal information such as their address, phone number, parent's or guardian's name
- Sharing or posting information about staff or other students, which these staff or other students would reasonably expect to be private
- Purporting to act on behalf of, or impersonate, the Division, its staff and other students
- Using the Division's network to post any material on the internet, newsgroups, bulletin boards, chat rooms, blogs or other public forums except as expressly authorized by the School Division
- Any non-school related online activity on a Division owned or personal device that negatively impacts network performance or others' use of the systems
- Unauthorized access to, or distribution of confidential or proprietary material of the Division
- Distributing unsolicited, non-school related email. (e.g. spam or chain mail)
- Sending, displaying or downloading offensive messages or pictures
- Using obscene language, harassing, insulting or attacking others, maligning or defaming the Division, its employees, its students or the St. James-Assiniboia community
- Sending fraudulent or anonymous messages
- Deliberately accessing, downloading, creating, storing, transmitting or printing sexually explicit or discriminatory content, or inappropriate content that contains obscene or objectionable material, including files or messages that are vulgar or that contain profane language or degrade others
- Downloading and/or installing unauthorized software on workstations or other Division owned devices
- Deliberately bypassing, attempting to bypass or disabling any workstation or network level security measures IT management measures
- Willfully damaging computers or any attempts to alter, damage, congest or destroy data on the division's network– such instances include, but are not limited to:
    - knowingly distributing or propagating files that may introduce a virus to the system

  - denial of service attacks
  - unauthorized access to any information or systems on the network

B. Student Safety

Ensuring student safety while accessing the internet access is the shared responsibility of Division personnel, parents/guardians and students.

Network and internet access measures, in addition to staff and student training and procedures are in place to encourage safe and ethical use of the Internet. The School Division employs the use of web content-filtering software to support our educational goals and initiatives (e.g. conducting research, communicating for legitimate school or educational activities).

Use of technology and communication resources by students will take place in settings supervised by instructional staff. Teachers will guide students toward appropriate online materials to ensure that all students are utilizing the Internet in a manner in line with the mission of the School Division.

Students and parents/guardians (for students under 18 years of age) are required to annually complete and sign the Division's Acceptable Use Agreement prior to receiving access to the Division network. (IJNDC-E-1)

In order to comply with The Freedom of Information and Protection of Privacy Act (FIPPA), the School Division requests consent annually from parents or students to post or publish photos of students, examples of student work and information on various public forums and media outlets. (IJNDC-E-1)

C. Student Owned Devices

In the classroom, cellphones (including smartwatches) can interfere with a student's ability to focus and learn effectively. Guidelines to limit cell phone use during school hours to help reduce distractions and support student learning are as follows:

- For K-8 Students: Cell phones are not to be used during school hours while on school property, including breaks and lunch.
- For Grades 9-12 Students: Cell phones are not to be used during class time, but can be used during breaks and lunch, or under direction by a teacher with the understanding that such use is restricted to supporting curricular pursuits in the classroom.
- For K-12 Students with Specific Educational or Medical Needs: Cell phone access will continue as outlined in Student Specific Plans.

Students are permitted network access only to the secure wireless network using their Division-supplied access credentials. Students are not permitted to connect personal devices to the wired network.

Students accessing the internet on personal devices using the Division WiFi network will be provided with filtered internet access. Beyond this safety measure, parents should be aware that the School Division will not be responsible for supervising student internet access on personal devices outside of in-class use.

The School Division assumes no responsibility for the loss, damage or theft of any student-owned device; nor will the Division be liable for the loss of any data on a student owned devices due to any technical or other difficulties.

Division IT staff will only provide direction for students to connect to the secure wife network. Division IT Staff will not provide technical support or other services for student-owned devices.

All rules and procedures of this policy also apply to student-owned devices accessing the School Division network.

D. Privacy Notice

The St. James-Assiniboia School Division network is intended for educational or research purposes. As such, students should have no expectation of privacy when they are using Division technology or networks, even if students are using their own devices. The Division will own all data and information that is stored on or transmitted by Division technology or networks.

E. Social Media & Other Interactive Online Services

Students will be held accountable for any information posted on social media sites or any interactive online services if it negatively affects the School Division or others, using either Division-owned or personal devices.

Please refer to Exhibit IJNDC-E-2 for Guidelines for Safe Student Use of Social Media.

F. Enforcement of Policy

Students will be responsible for their actions and are encouraged to report any unauthorized or inappropriate use immediately to their teacher or school administration.

Failure to comply with the rules and procedures set out in this policy as well as the Student Conduct (JK) policy may result in temporary or permanent loss of access as well as other disciplinary action as necessary.

The Division reserves the right to:

- monitor online activities by students and to access, review, copy, store or delete any electronic communication or files and disclose them to others so that the Division can administer and operate the Division networks; conduct investigations into violations of this or other policies; comply with Division duty, under provincial legislation, including the duty of the Division to provide a safe school environment, under the Public Schools Act

- access student user accounts in cases where there is reasonable cause to suspect misuse of the system
- enact disciplinary consequences as a result of inappropriate student actions as deemed by the Division
  - Disciplinary consequences may include temporary or permanent loss of network access, and/or legal action. Principals are to refer to JKD-R (Safe and Caring Schools: Appropriate Interventions and Disciplinary Consequences).