#113585

GBEF
GBEE

Employee Use of Technology and Electronic Communication

The St. James-Assiniboia School Division network is intended for educational or research purposes and for conducting valid school or divisional business.

Employees who have use of the Division's network and related resources are responsible to:

- take reasonable measures and act responsibly to protect the equipment from misuse, loss, theft or damage and promptly notify the Division in any such event
- ensure that confidential information of the Division is protected
- accept ultimate responsibility for their actions in accessing Division technology and communication resources
- use good judgment at all times and to respect the rights and privacy of other technology users
- follow generally accepted network etiquette rules, including using appropriate language and content in all correspondence or communications
- abide by all applicable copyright and intellectual property laws
- use only the Divisional accounts (e.g. network login, e-mail) assigned to them by the Division IT Department
- ensure all user IDs and passwords for Divisional accounts remain confidential
- close all Internet browser windows and log off the Divisional network when not directly using a computer or mobile device
- not independently attempt to modify settings, install software or uninstall software previously installed by the Division IT Department
- ensure that any hardware and software additions and change requests are processed, authorized and installed through the Administrator of Technology. All installations and changes to systems must be performed and/or authorized by a member of the Information Technology (IT) Department
- connect personal devices only to the secure wireless network in the interests of protecting the integrity and reliability of the Division's corporate network
- access only Internet sites with content appropriate for a school environment
- ensure they maintain a personal backup of their files in addition to the Division's central backup of all end user files
- 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
- understand accept the consequences of inappropriate use of technology, as outlined in this policy

The following list details examples of prohibited activities based on employee 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
- Employing Division technologies for commercial or political purposes (e.g. promoting and/or advertising commercial events, promoting a political party or candidate)
- Any non-work 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-business 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, storing, transmitting or printing inappropriate content that contains obscene or objectionable material, including files or messages that are vulgar or sexually explicit, 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
- 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

Use of Personal Devices

Staff may use cell phones for instructional purposes or as directed by administration to support the overall operation of the school. Personal cell phone use is limited to breaks and lunch periods. Staff with medical needs or emergencies that require cell phone use are required to inform administration to ensure exceptions are handled appropriately while maintaining overall cellphone guideline consistency.

Privacy Notice

- The St. James-Assiniboia School Division network is intended for educational or research purposes and for conducting valid school or divisional business.

- If any employee chooses to use Division provided technology and communication systems for purposes other than work:
    - He/she does so with the understanding that all that information accessed and\or stored on the Division network and hardware is the property of the Division and may be viewed by the employer
    - Such use complies with this policy and does not interfere with work duties, nor in a manner that harms the interests of the Division, its staff or its students, or is in violation of any laws.
- Employees should not have any expectation of privacy with respect to any equipment or technology that the Division provides. This would also include employee use of personal devices accessing the Division WiFi network. If an employee requires a private means of internet access and communication, they should only use a personal electronic device not connected to the Division's network.

Enforcement of Policy

The Division reserves the right to:

- Monitor staff use of Division technologies for the purpose of:
    - administering and operating its networks and related systems
    - conducting investigations into violations of this or other policies
    - online activities by employees and to access employee user accounts in cases where there is reasonable cause to suspect misuse of the system or unlawful activity
    - productivity concerns, and the ability to perform duties the employee is being paid by the employer to perform
    - disclosure of the employer's confidential information, as well as infringements on individual staff and student policy
    - preventing defamatory statements and harassment by employees (which contravenes workplace safety and health legislation)
    - protecting the employer's reputation
    - complying with the Division's legislated duties.
- To access staff user and email accounts in cases where there is reasonable cause to suspect misuse of the system or violation of Division policy.

Violations of this policy will result in appropriate discipline, which may include temporary or permanent loss of access, suspension or termination of employment, and/or legal action.