Rolling River School Division

ADMINISTRATIVE PROCEDURE

GBCF – ACCEPTABLE EMPLOYEE USE OF TECHNOLOGY AND ELECTRONIC COMMUNICATION

Employees refers to all RRSD employees, contract employees, and the Board of Trustees.

Rolling River School Division (RRSD) recognizes that new technologies in today's society can enhance learning environments by providing employees ways to create, collaborate, communicate and think critically.

To support the Division's commitment in the use of information technology and enhance the digital learning environment across the Division, employees are provided with access to computers, devices, networks and other technology resources. The Division will ensure that interactions within this learning environment contribute to a safe and positive school climate.

This policy and regulation applies to:

- All employee use of School Division computers, devices, networks and facilities owned, or leased and operated by the Division.
- Employee-owned devices used to access the Division network and related resources.

To comply with The Freedom of Information and Protection of Privacy Act (FIPPA), the School Division requests consent from employees to post or publish photos and personal information on various public forums and media outlets.

Employees are responsible for their activity, behaviour and communications over the network and are expected to comply with all Division policies related to the respectful, responsible, ethical and lawful use of technology.

Rolling River School Division's (RRSD) 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:

- act responsibly and protect the equipment from misuse, loss, theft or damage and promptly notify the Division/School Administration in any such event;
- obey network and Internet limitations and restrictions put in place by the Division;
- ensure that confidential information of the Division is protected;
- accept 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;
- obey 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;
- maintain settings and software previously installed by the Division IT Department; do not modify or uninstall software;
- ensure that any hardware and software additions and change requests are processed, authorized and installed through the Coordinator of Instruction, Curriculum, and 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;
- 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 through the Coordinator of Instruction, Curriculum, and Technology;
- accept the consequences of inappropriate use of technology, as outlined in this policy;

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.
- Releasing personal information such as address, phone number, or names.
- Sharing or posting information about others including employees and students.
- Purporting to act on behalf of or impersonate the Division or someone else.
- 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 Rolling River School Division 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 implemented by the Division.
- Any attempts to alter, damage, congest or destroy data on the division's network 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

Privacy Notice

- Rolling River School Division's network is intended for educational or research purposes and for conducting valid school or Divisional business.
- The Division owns all data and information that is stored on or transmitted by Division technology or networks.
- Employees have no privacy when they are using Division technology or networks even if employees are using their own devices.
- The Division will 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 and email 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 that 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 privacy.
    - 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.

Enforcement Policy

Employees are responsible for their actions and are encouraged to report any unauthorized or inappropriate use immediately to their supervisor or school administration.

Failure to comply with the rules and procedures set out in this policy may result in disciplinary action as necessary.

Date Adopted: October 9, 2019