# Prohibited Use of District Technology Regulation

## 3350-22 | Prohibited Use of District Technology Regulation

Date Approved: October 06 2017
Date Amended:

---

This regulation applies to all school district related use of district technology or personal devices, including off-campus activities.

**Prohibited Uses of Electronic Information Resources**

1. It is prohibited to use district technology or networks (including email):

- For illegal, inappropriate, immoral or other purposes that are inconsistent with district values, principles and policies;
- For bullying or harassment of any other users or any other persons;
- For purposes which would bring the reputation of the district into disrepute;
- To facilitate use of the district network for commercial or for-profit purposes;
- To solicit products or services that are incompatible with the mission of the district.
- For distribution of hate mail, discriminatory remarks and defensive or inflammatory communication material;
- For the unauthorized or illegal installation, distribution, reproduction, use or plagiarism of copyrighted materials;
- For the use or distribution of inappropriate language or profanity on the network;
- To create internet identities to impersonate another person; or
- To represent or identify oneself inaccurately and/or dishonestly when participating in chat groups, making postings on groups, sending email, or otherwise communicating using district technology or networks

2. Waste of Time and District Resources:

- Users may not deliberately perform acts that waste district resources or unfairly monopolize resources to the exclusion of other users, including sending mass mailing of emails such as chain emails and the use of music or video sharing sites.
- Users shall not spend excessive or inappropriate amounts of time on the internet, including playing games, engaging in on-line chat groups, social networking, printing multiple copies of documents for personal use or otherwise creating network traffic that does not serve the district.
- During work hours employees will always restrict their use of district networks to those activities related to their duties with the district.

3. It is unacceptable for any user to attempt to log on as any other person or user without the permission from the Superintendent or designate. The only exceptions are for troubleshooting access to a system by Information Technology Department personnel or providing access pursuant to an investigation.

4. Audio files, video files and pictures with significant storage requirements and/or copyright restrictions may not be downloaded unless they are for educational purposes or otherwise approved by a principal or supervisor.

5. Users may not misuse software, such as to:

- Copy software for use on their home computers unless proper authorization is given by the Superintendent or designate;
- Provide copies of software to any other user unless authorization is granted by the Manager, Information Technology;
- Modify, revise, transform, recast or adapt any software; or
- Reverse engineer, disassemble or decompile any software.

Exceptions to these restrictions may occur for educational purposes with prior authorization of the Director of Instruction, Educational Transformation or designate

6. Unless expressly authorized by the Superintendent or designate, sending, transmitting or otherwise disseminating proprietary data, trade secrets or personal or confidential information of the district is strictly prohibited. Unauthorized dissemination of information may result in discipline, civil liability and/or criminal penalties under Federal or Provincial laws.

**Security of Electronic Information Resources**

1. Users may not delete, alter, or copy files, passwords or data belonging to another user without first obtaining permission from that user. This does not apply where a group of users share a common electronic workspace where it is generally accepted and understood that modification of those files is part of their role with the district.
2. The district employs several shared electronic workspaces where data should not be modified.
3. Users may not investigate the actions of other users (for example, by unnecessarily and inappropriately reviewing emails or files).
4. A user's ability to connect to various computer systems through a network does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operator of those systems or by the Director of Instruction, Information Technology or designate.

**Encryption Software**

1. No user is permitted to install or utilize encryption software on any district technology without first obtaining written permission from the Secretary-Treasurer or designate.

**Reporting of Inappropriate Internet Sites or Other Inappropriate Use of District Networks**

1. The procedure to follow when a user has identified that this regulation is not being followed is to do at least one of the following:

- Notify a teacher;
- Notify a school principal(s);
- Notify a supervisor; or

- Notify the Information Technology Department.

2. Anyone who becomes aware of an inappropriate internet site must advise the Information Technology Department, or any principal or supervisor, so that appropriate steps may be taken to either block access or restrict access to the site.

3. Requests to have unblocked sites that are incorrectly blocked should be made to the principal or supervisor. The district has implemented a web content filter that errs on the side of child safety so it is reasonable to expect that some sites will be incorrectly blocked. The request process to have sites unblocked is intended to be informal and quick.

**Breach of Policy/Regulation**

Any violation of the Acceptable Use of Technology Policy or Regulations may result in:

1. Loss of access privileges;
2. Loss of volunteer positions;
3. Student disciplinary measures;
4. Employee disciplinary action (up to and including termination); and
5. Legal action including actions taken by the district, by persons unrelated to the district, and/or criminal prosecution

**Related Policies and Regulations:**

| | |
|---|---|
| Bylaw #7 | Freedom of Information/Protection of Privacy Bylaw |
| 1170-10 | Copyright Regulation |
| 1410 | District Code of Conduct Policy |
| 3350 | Acceptable Use of Technology Policy |
| 3350-10 | User Accounts and Passwords Regulation |
| 3350-20 | Acceptable Use of District Technology |
| 3350-25 | Bring Your Own Device Regulation |
| 3350-30 | Technology and Instruction Regulation |
| 3350-40 | Data Security and Privacy Regulation |
| 3350-50 | District and School Websites Regulation |

| | |
|---|---|
| 4320-10 | Bully and Harassment Regulation |
| 6710 | Records Management Program Policy |