Data Security and Privacy Regulation

3350-40 | Data Security and Privacy Regulation

Date Approved: October 06 2017
Date Amended:

The district will provide reasonable monitoring and supervision of all schools' and administrative buildings' networks and technology in order to maintain data security and privacy.

Collection of Personal Information

- Personal information of a user is stored on the email server and in logs monitoring internet use. In accordance with section 26(b) of the *Freedom of Information and Protection of Privacy Act*, the collection of this data is directly related to the programs and activities of the district.
- The data collected from internet access will be:

- Time and date stamp of the resource accessed;
- The resource accessed;
- The user account of the resource accessed (where possible); and
- The IP address of the district technology or personal device used to access the resource.
    - The purpose of the collection of this data is primarily for performance monitoring to appropriately manage district technology and networks. This information can and will also be used to block content on the internet that is not appropriate for use in the public school system.
    - The data collected from emails is a record of all emails sent from and received at a district email address.
    - In accordance with section 27(2) of the Freedom of Information and Protection of Privacy Act, any questions about the collection of this personal information should be directed to:
        - Secretary-Treasurer,
          634 6th Avenue East
          Prince Rupert BC V8J 1X1
          250-624-6717

- At any time, an employee may request in writing to the Secretary-Treasurer a copy of all records directly attributable to their own user account. The district agrees to provide copies as set out in *Bylaw #7 Freedom of Information/Protection of Privacy*.

Monitoring of Email and Internet Use

- The district employs several technologies to proactively monitor use of the internet to protect users and devices. Part of this monitoring includes collecting information about the sites visited by individual users. This monitoring technology also permits control on which sites may be blocked or accepted at a user's device.
- Employees of the district have a reasonable expectation of privacy for their email and access to n the internet. Routine monitoring of access to the internet shall be performed, if reasonably practicable and

appropriate, in as anonymous a fashion as performance of the overall networks may allow. Logs of internet use will typically not be maintained for more than 365 days except as required by law or unless a review or an investigation has been initiated.

- Students do not have a reasonable expectation of privacy on their access to the internet. The monitoring of internet use for students may be reviewed continuously, and monitoring results may be shared amongst teachers and principals directly responsible for the education of the student.
- All other users who are not students or employees have no expectation of privacy on their access to the Internet. The district may choose to monitor and control internet access, including sharing the monitoring information as it sees fit.
- The district may actively monitor the internet use or emails of a specific user when there are reasonable grounds to indicate that the Acceptable Use of Technology Policy or Regulations may be, are being or have been violated. Active monitoring of an individual user's internet access will normally only be performed after notifying the user that this monitoring is occurring, unless such notification would compromise a school district, law enforcement or other investigation. Active monitoring will always be specified with a definitive start date and time and end date and time, and will never be performed for more than 31 consecutive days.

Software Installation

- The Superintendent or designate may authorize the application of software or hardware that may restrict or track access of inappropriate material.
- Only district owned software programs (including free and/or open source software and hardware) may be installed on district technology unless authorized in writing by the Manager, Information Technology or designate. The Information Technology Department may remove any unauthorized software from district technology without prior warning to the user.
- No user is permitted to install or utilize encryption software on any district technology or network without first obtaining written permission from the Secretary-Treasurer or designate.
- The district may implement third party encryption keys and passwords where district personnel may not have the direct ability to decrypt information. Implementation of these kinds of encryption keys may only be authorized by the Secretary-Treasurer or the Superintendent.

User Information and Data

- The district may occasionally require new registration and account information from users to continue existing services or to provide new services. The district will never use email to ask for passwords or personal user information; any email asking for such credential information should be immediately brought to the attention of a teacher, principal, supervisor and/or the Manager, Information Technology.
- Although the district has implemented disaster recovery policies for application, file and email servers, it is the responsibility of individual users to ensure their personal work is stored on district file and email servers so that it will be backed up. Users are responsible for backup of all other data critical to themselves. All backups of systems must be stored in a secured location. Because backups may contain personal information, the loss of any backup media must be immediately brought to the attention of the Secretary-Treasurer.
- The district has enabled mobile technology to access email and servers. There are access controls that allow a secure remote wipe of mobile technology that must be accepted before the mobile technology is permitted to connect to district networks. In the event that mobile technology that is connected to district networks is misplaced or stolen, the user must bring this to the attention of the Information Technology Department so that appropriate measures can be taken to remotely disable access or wipe the device.
- Intentional defeating of remote wipe access controls on mobile technology (personal or district owned)

connected to district networks will result in immediate suspension of access to district networks.

Related Policies and Regulations:

Bylaw #7	Freedom of Information/Protection of Privacy Bylaw
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 Regulation
3350-22	Prohibited Use of District Technology Regulation
3350-25	Bring Your Own Device Regulation
3350-30	Technology and Instruction Regulation
3350-50	District and School Websites Regulation
6710	Records Management Program Policy