Keewatin Patricia DISTRICT SCHOOL BOARD	Procedure Section: **Business and Administrative Matters** Procedure Name: **Responsible Use of Learning Technology and Data**	**600** **618**

PROCEDURE

Responsible Use of Learning Technology and Data

These procedures set out the responsibilities of the Keewatin-Patricia District School Board (KPDSB), schools, and users of learning technology. Also included are examples of unacceptable uses and consequences for inappropriate use.

Using Learning Technology

1. All users of KPDSB learning technology resources are responsible for appropriate and ethical behaviour at all times.

2. Employees will promote the ethical use of technology resources and will provide guidance, support, supervision, and instruction to students as they access educational resources.

3. Employees must be aware that the data they create with KPDSB learning technology and on KPDSB-managed systems remains the property of the KPDSB.

4. All users must be aware that the KPDSB cannot guarantee the confidentiality of information stored on any network or technology device belonging to the KPDSB because of the need to protect the KPDSB's information and network.

5. All KPDSB technology supplied to, or used by, KPDSB employees, Trustees, students, and volunteers remains the property of the KPDSB which gives the KPDSB the right to monitor any and all activity on its technology and systems.

6. Users are responsible for exercising good judgement regarding reasonable personal use. Users must not have any expectation of privacy when storing personal information on KPDSB networks or KPDSB-owned technology.

7. For security and network maintenance purposes, authorized individuals within the KPDSB may monitor technology, equipment, systems, and network traffic at any time. The KPDSB reserves the right to audit technology, networks, and systems on a periodic basis to ensure compliance with this procedure.

8. All users must keep passwords secure and not share accounts. Authorized users are responsible for the security of their passwords and accounts.

9. Certain web applications may require the use of multi-factor authentication as configured by the KPDSB.

10. All users must ensure that any information posted to the Internet is consistent with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

11. Under MFIPPA, all electronic records are subject to a Freedom of Information request.

12. At no time will KPDSB technology be used for individual commercial purposes or personal financial gain. The KPDSB retains ownership, control, and copyright over anything created, composed, or otherwise developed using KPDSB technology resources.

13. The KPDSB assumes no liability for any direct or indirect damages arising from the user's connection to the internet or misuse of technology. The KPDSB is not responsible for the accuracy of information found on the internet and only facilitates access and dissemination of information through its systems.

Board Issued Equipment

1. Staff may be assigned laptops, Chromebooks, tablets, iPads, and other electronic computing equipment. Schools also have sets of computing devices such as laptops, Chromebooks, and tablets. Users will be required to complete a User Agreement that communicates the roles and responsibilities of KPDSB staff as they use board-issued technology.

2. In the event that an employee terminates employment with the KPDSB, their employment is terminated by the KPDSB,or they are on extended leave from KPDSB, the employee will return the equipment on or before their last day.

3. The employee is responsible for the set-up of equipment off site. The Learning Technology (LT) Department will provide hardware and software support during regular office hours. The LT Department will not provide off site support at any time.

Prohibited Uses

1. Posting student work, photographs, and/or video images on any public website without prior written consent from the student's parent or guardian. **Form Consent to Release Personal Information**

2. Posting student's personal information such as class lists, marks, and demographic information in a non-secured environment.

3. Copying or downloading copyrighted and/or intellectual property materials such as movies, music, and images.

4. Using the learning technology during the school or workday for purposes unrelated to learning or work.

5. Accessing illegal, harassing, obscene, pornographic, racist, libelous, threatening, promoting physical violence or sexually explicit resources.

6. Using electronic mail to send obscene, threatening, harassing, libelous, discriminatory, or inflammatory messages.

7. Installing unauthorized software.

8. Causing disruption of the internet and/or intranet.

9. Using KPDSB technology at any location for the purposes of bullying and/or harassing.

10. Damaging the work of an individual or organization.

11. Using inappropriate language or being disrespectful when communicating over the internet or through electronic mail.

12. Accessing private or personal information without prior authorization.

13. Using the internet or email accounts in a manner that is not consistent with the mission of the KPDSB, misrepresents

Compliance

1. All users are expected to comply with this procedure. Failure to comply with this procedure could result in disciplinary action.

2. Appropriate legal authorities may be contacted if there is any suspicion of illegal activity.

3. In the event that an employee has violated this procedure, the employee will be provided with notice of such violation. An employee's access to the KPDSB's learning technology may be denied, restricted, or suspended and additional disciplinary action may be taken up to and including dismissal.

Device User Information

The following communicates the roles and responsibilities of Keewatin-Patricia District School Board (KPDSB) staff hereinafter referred to as the User, that have been assigned a Laptop, Chromebook, iPad, or other device(s) hereinafter to as "the Device".

1. Usernames and passwords are unique to each user. The User must not share their usernames nor passwords. The confidentiality of login credentials is the user's responsibility and if there is a compelling need to disclose your password with anyone, including a LT technician for a temporary event, it must be changed immediately afterward.

2. The Device is the property of the KPDSB.

3. The Device is a tool to be used by the User to support their respective positions. The Device is configured with Board owned/licensed software and remains the property of the Board. The User must use reasonable care in the use and physical maintenance of the Device

4. The Device may be portable and contain private and confidential information. It is the responsibility of the User to ensure that the security and integrity of any data contained on the Device will not be compromised. While not all-encompassing, the following are expectations to ensure the confidentiality of any data:

    a) Access to the Device is restricted to KPDSB staff.

    b) The Device must be stored in such a way that it will be difficult to misappropriate either the physical device or the data stored within it.

    c) When used in a place where other persons could view the screen, reasonable care should be taken to protect confidential information.

    d) Any action or activity that could make confidential information available to non-authorized persons must be avoided.

    e) When using portable storage devices (i.e., USB keys, portable hard drives, etc.), confidential data is to be kept secure.

    f) The Device is configured to require a password to log in.

5. Data stored on the device is outside of the KPDSB's server environment. Keeping a backup of that data is the responsibility of the Device User.

6. Any unlawful or prohibited use of the Device as defined by Procedure 618 – Responsible Use of Learning Technology and Data and/or Policy 706 – Employee Code of Conduct may result in disciplinary action.

Windows Laptops

1. Laptops have Microsoft Windows installed and are configured to automatically download and install Microsoft Windows updates. The User may need to monitor their laptop so that when updates have been downloaded, they are installed in a timely manner.

2. XDR (Extended detection and response) security software is installed on the Windows laptop by the KPDSB LT Department. The XDR software is configured centrally and will not allow an end-user to change, defeat, disable, or uninstall the application.

3. Laptops are configured with an application called Kaseya which provides the LT Department access to the laptop. KPDSB LT Technicians will have access to the laptop for routine maintenance, updating, troubleshooting, and configuring of the machine. Any personal information contained on the machine could therefore be viewable by LT Technicians.

4. Applications used on the laptop will be kept up to date by the LT Department as best as possible. The user is responsible to check to make sure they are up to date. Sometimes the LT Department will FORCE updates/reboots when critical. It is important that Users frequently save their work so that forced updates do not result in work potentially lost.

Chromebook Laptops

1. Chromebooks are joined to KPDSB's K12 Google Domain and must not be reconfigured.

2. Chrome OS updates will automatically download to the Chromebook. Therefore, the User may need to reboot the device to install the latest updates. Sometimes the LT Department will FORCE updates/reboots when critical.

3. Google Workspace for Education is used by the KPDSB LT Technicians to manage, maintain, and configure the Chromebooks.