# ACCEPTABLE USE OF DIGITAL TECHNOLOGY

## BACKGROUND

When used responsibly, technology can facilitate collaboration between students, educators, and parents; provide access to a wide variety of online resources, enhance engagement, and amplify student learning. The district recognizes its responsibility to provide guidance in responsible technology use. This Administrative Procedure ensures the appropriate and legal use of district technology to support teaching, learning, and administrative functions. It emphasizes responsible digital citizenship and the protection of personal information.

## PROCEDURES

1. **Expectations for all users:**

1.1. Users must comply with all relevant district, provincial and federal policies, procedures, and guidelines.

1.2. Users will conduct themselves in a respectful, ethical, legal, and responsible manner and use technology services and platforms only for educational and administrative purposes.

1.3. Users are responsible for all activities carried out through their user accounts, including material they choose to access, send, or display.

1.4. District technology, including but not limited to, email services, internet use and data stored on district networks are District property and may be inspected or monitored at any time.

1.5. Users will only access authorized district services, digital content, and licensed software. Users will not access, store, or distribute inappropriate material which includes pornography, threatening, offensive, or obscene material.

1.6. Users will promptly report any accidental access to inappropriate messages or material to the appropriate school or District employee (School Principal or District Administrator).

1.7. Users will ensure that they limit their use of digital technology to those tools in compliance with the Freedom of Information and Protection of Privacy Act (FOIPPA), current Terms of Use of the specific tools, and the provisions of this Administrative Procedure.

1.8. Users will not use someone else's account or identity online or distribute false defamatory information.

1.9. All passwords protection mechanisms available on portable technology must be activated and utilized consistently and to the greatest extent possible. Users will maintain digital security, keep passwords private, and deploy industry standards in password selection.

1.10. Users will seek consent before taking or sharing photos or videos of others.

1.11. Users shall not engage in any activity harmful to district technology or attempt to vandalize it.

1.12. Users who notice security threats will immediately report them to the appropriate school or district employee.

## 2. Consequences for misuse

2.1. Non-compliance with this Administrative Procedure may result in restrictions, suspensions, or revocation of technology privileges.

2.2. Violations may be reported to law enforcement authorities and could lead to criminal investigations or charges.

## 3. Staff Communications

3.1. Human Resources will ensure staff users review and sign the Staff Technology User Agreement upon hire (Appendix A). New staff members will be provided Freedom of Information and Protection of Privacy Act (FOIPPA) training.

3.2. Principals will review this procedure annually.

3.3. When selecting digital tools, staff will refer to the District privacy portal to verify that the tool has been reviewed and approved through a comprehensive privacy impact assessment.

3.4. Staff wishing to use tools that have not been reviewed by the District must seek Principal approval. The District privacy portal can be consulted for further guidance regarding tool selection.

3.5. Parental consent for the use of digital technology is obtained annually through the start of year consent package.

3.6. Staff will annually review the appropriate Student Technology User Agreement (Appendix B) with their students and if they wish, have students sign the agreements.

3.7. (Appendix C) provides guidelines for professional social media communication among district employees and between staff and students. Student-to-student communication via social media is addressed in each school's code of conduct and Student Technology User Agreements (Appendix B).

## 4. Personal Electronic Devices

4.1. Users may bring personal electronic devices (PEDs) to perform school/work related duties. It is expected that users comply with all relevant district, provincial and federal policies, procedures, and guidelines when opting to bring their own electronic devices into New Westminster Schools and District offices.

4.2. The security and storage of PEDs is the sole responsibility of the owner/user. The District assumes no responsibilities for the safety, security, loss, theft, damage, repair, or replacement that may occur to PEDs brought to the school or worksite.

4.3. (Appendix D) provides guidance related to personal electronic devices and the associated Bring Your Own Device initiative for students.

**4.4.** Parents and Students participating in BYOD must sign the BYOD Responsibility Contract found in (Appendix E).

**Definitions**

**District technology**: a broad range of digital communication services, platforms, and information including hardware, software, district networks.

**Users**: anyone using or accessing district technology, including students, staff, parents, and guests.

**Personal electronic devices**: user-owned electronic devices.

***References:*** *Sections 22, 65, 85 School Act*
*Freedom of Information and Protection of Privacy Act*
*Freedom of Information and Protection of Privacy Regulation*

*NOTE: Administrative Procedures 140 replaces AP 145 - Use of Personal Communication Devices & AP 146 - Responsible Use of Electronic Social Media*

***Adopted: May 28, 2019***
***Revised: August 2, 2023***