AP – 4.14 ELECTRONIC TECHNOLOGY SYSTEMS USE

1. PURPOSE

To establish clear guidelines for the appropriate and responsible use of the School District's electronic technology systems, ensuring these resources support educational and administrative goals while maintaining a safe, secure, and respectful digital environment.

2. SCOPE

This procedure applies to all employees, students, contractors, and volunteers who access or use the School District's electronic technology systems, including but not limited to:

- Internet access
- District email systems
- MyEDBC and other student information systems
- Computer hardware and software
- Mobile phones and tablets
- Network infrastructure and cloud services
- Any other equivalent technology

3. POLICY STATEMENT

- Access to District technology resources is a privilege, not a right, and may be revoked if misused.
- Employees and students should have no expectation of privacy when using District-provided technology or systems. All communications and data stored on District devices may be monitored and accessed by authorized personnel.
- The primary purpose of District technology is to support educational, administrative, and operational functions.

4. ACCEPTABLE USE

Use of District technology is acceptable when it:

- Is legal, ethical, and aligns with the goals and professional standards of the School District and the BC College of Teachers.
- Supports the educational mission of the District and enhances student learning or staff efficiency.
- Respects the rights, privacy, and dignity of other users.
- Maintains the integrity and security of the District's technology systems.

5. Unacceptable Use

The following activities are considered unacceptable and are strictly prohibited. This list is ***not exhaustive***, and other actions that compromise the security, integrity, or ethical use of District resources may also be deemed unacceptable.

a. Inappropriate Content and Behavior

- Sending or accessing offensive, obscene, profane, sexually explicit, defamatory, malicious, abusive, threatening, racially offensive, or otherwise inappropriate content.
- Creating, sending, or forwarding messages that fail to meet professional standards of language and tone.
- Engaging in cyberbullying, harassment, or any form of discriminatory behavior.

b. Unauthorized and Misuse of Resources

- Using District systems during work hours for non-work-related purposes that do not align with the employee's duties.
- Inappropriate distribution of personal or confidential information, particularly related to students.
- Using District systems to pursue personal financial gain or any commercial ventures (e.g., gambling, online sales, etc.).
- Accessing or distributing unlicensed software or materials.
- Intentionally obscuring the origin of any message, such as spoofing email addresses.
- Using District resources for political, union, or non-approved organizational purposes.

c. Network and System Violations

- Attempting to bypass security protocols or subvert system protections.
- Vandalizing or damaging technology resources (e.g., spreading malware, viruses, or disabling systems).
- Over-utilizing network resources (e.g., streaming media not related to education or work duties).
- Participating in network games, chat rooms, or streaming services that consume significant bandwidth without educational or administrative justification.
- Excessive personal use of District resources, including bandwidth, storage space, or printing.

6. Ownership of Electronic Communications

- All data and communications created, sent, or stored on District-owned equipment (including email) are property of the District.
- The District reserves the right to monitor and access any material on its systems without prior notice.
- Employees and students should not expect privacy when using District technology, including emails, files, or online communications conducted via District accounts.

7. Security and Confidentiality

- Users are responsible for maintaining the security of District systems by:
    - Using strong passwords and keeping them confidential.
    - Logging out of systems when not in use.
    - Reporting any security breaches or suspicious activity to IT personnel immediately.
    - Handling confidential data (especially student information) responsibly and sharing it only with authorized individuals.

8. Consequences for Violations

- Violations of this procedure may result in progressive disciplinary action, including, but not limited to:
    - **For Employees:** Verbal or written warnings, suspension, or termination.
    - **For Students: Loss** of technology privileges, suspension, or other disciplinary measures.
    - **For Volunteers/Contractors:** Revocation of access privileges and potential termination of contracts.
- Note: Illegal activities will be reported to law enforcement as appropriate.

9. User Responsibilities

- All users of District technology are expected to:
    - *Use District technology ethically and responsibly.*
    - *Respect the rights and privacy of others.*
    - *Report any technical issues, security breaches, or inappropriate content to school administrators or IT staff.*
    - *Participate in training sessions and review updates to District technology policies as required.*

10. References

- BC Freedom of Information and Protection of Privacy Act (FIPPA)
- BC College of Teachers Standards
- BC School Act