RESPONSIBLE TECHNOLOGY USE

Background

Peace River School Division (PRSD) provides technology resources to students and staff to enhance teaching, learning, and operational efficiency. Use of Division-provided technology is a privilege, and not a right. Users are expected to act responsibly, ethically, and in compliance with the Education Act (Alberta), Access to Information Act (ATIA), Protection of Privacy Act (POPA), and Division policies and procedures, including cybersecurity and privacy best practices.

Definitions

PRSDnet refers to the Division's networked technology environment and all associated digital resources provided to students and staff. This includes, but is not limited to, Internet access, wired and wireless networks, computers and devices, user accounts, email and communication systems, and Division-approved software and online services.

Procedures

1. User Responsibilities
    1.1. PRSDnet users are expected to conduct themselves when using PRSDnet with the same respect and responsibility required in the classroom or school environment.
    1.2. Communications on PRSDnet are often public in nature.
    1.3. All school rules for behaviour and communication apply when using PRSDnet, including digital communications and online conduct.
    1.4. Violations of PRSDnet responsibilities may result in suspension or loss of access privileges and could lead to disciplinary or legal action.
2. Purpose and Access
    2.1. PRSDnet is provided to staff and students to support research, learning, collaboration, and communication related to school work and Division operations.
    2.2. Access is granted only to users who agree to act in a considerate, responsible, and lawful manner.
    2.3. All users must sign or electronically agree to a PRSDnet Responsible Use Agreement before being granted access. Parent/guardian permission is required for students.
    2.4. Inappropriate or unauthorized use of PRSDnet is strictly prohibited and will not be tolerated.
    2.5. The Superintendent or designate may disable, limit, or suspend a user account at any time to protect PRSDnet security, investigate suspected misuse, or enforce PRSD policy.

3. Individual Use Requirements

   3.1. PRSDnet accounts must be used in support of education, research, or Division operations.

   3.2. Use of other organizations' networks or computing resources must comply with their rules and policies.

   3.3. Transmission of material in violation of Canadian or Alberta law (including copyright, threatening, hateful, or obscene content) is prohibited.

   3.4. Unauthorized commercial activity, product promotion, or illegal acts are strictly prohibited.

4. Digital Etiquette & Conduct

   4.1. Keep passwords and personal information confidential.

   4.2. Respect the confidentiality of others' information.

   4.3. Avoid disrupting PRSDnet services or interfering with others' work.

   4.4. Treat others' data with respect and avoid modifying or damaging their information.

   4.5. Comply with copyright and intellectual property laws.

   4.6. Access only authorized systems and resources.

   4.7. Not seek, transmit, or accept obscene materials.

   4.8. Use email responsibly, recognizing it is not private (see AP 140 Appendix – Email).

   4.9. Avoid profanity, racist comments, harassment, or offensive language.

5. Privacy and Monitoring

   5.1. Users have no expectation of privacy for anything created, stored, sent, or received on PRSDnet.

   5.2. PRSD may monitor PRSDnet activity for security and compliance purposes, in accordance with the Protection of Privacy Act (POPA).

6. Users must not deliberately waste or monopolize PRSDnet resources. Prohibited actions include:

   6.1. Sending mass mailings or chain letters.

   6.2. Printing excessive copies of documents.

   6.3. Creating unnecessary network traffic.

7. Software, Applications, and Extensions

   7.1. PRSD devices are configured so that users cannot install software, applications, or browser extensions. All installations are managed centrally by Division IT.

   7.2. Users must use only software, cloud services, and apps that have been vetted and approved by the Superintendent or delegate.

7.3. Use of unapproved personal cloud services (e.g., personal Dropbox, Google, etc.) is prohibited for storing Division data.

7.4. Copying, sharing, or bypassing licensing restrictions for software or apps is prohibited.

7.5. Attempts to bypass technical controls, alter device management settings, or install unauthorized tools are strictly prohibited.

7.6. Users who become aware of misuse, unlicensed software, or security concerns must report incidents to the Division IT team immediately.

8. Encryption, VPN, and Security Tools

8.1. Users may not install or use encryption software, Virtual Private Networks (VPNs), proxy tools, or tunneling services on PRSD devices or networks without prior approval from their supervisor or Division IT.

8.2. Any approved VPN connections must use Division-provided or Division-approved solutions and must comply with PRSD security standards.

8.3. Passwords, encryption keys, and security tokens used on PRSDnet devices must be known to the Superintendent or designate to ensure recoverability and compliance.

8.4. Users must immediately report any suspected security breach, lost/stolen device, or compromised credentials.

9. User Responsibilities for Personal Information & Privacy

9.1. All PRSDnet users handle personal information and are responsible for protecting it in compliance with the Access to Information Act (ATIA) and Protection of Privacy Act (POPA, Bill 33).

9.2. Do not collect or request personal information unless it is necessary for educational programming, school operations, or Division-approved purposes.

9.3. Always use PRSD-approved platforms (email, SIS, learning apps) for storing or transmitting personal information. Do not store Division data on personal devices or unapproved cloud services.

9.4. Share personal information only with authorized staff, parents/guardians, or service providers who have a valid educational need-to-know.

9.5. Before using an optional or high-risk digital tool with students, confirm that parent/guardian consent has been obtained.

9.6. Immediately report any suspected privacy breach.

10. Vandalism & Harassment

10.1. Any attempt to harm, modify, or destroy data, upload malicious software, or harass another user will result in account suspension and may lead to disciplinary or legal action.

11. Violations of this AP may result in:

11.1. Suspension or loss of PRSDnet access privileges.

11.2. Disciplinary action up to and including termination (for staff) or suspension/expulsion (for students).

11.3. Referral to law enforcement when required.

Adopted/Revised/Reviewed: SEP 2025