Rocky Mountain School District #6

DISTRICT PRACTICE 2700.2

STUDENT ACCEPTABLE USE OF DIGITAL TECHNOLOGY

DISTRICT PRACTICE:

This district practice outlines the School District's procedures to reduce the risks posed by internet usage as a starting point for promoting positive digital citizenship among students. The School District's expectations for student online behaviour are no different than for face-to-face interactions in school and are governed by Board of Education policies and government legislation. Successful, technologically savvy digital citizens live safely and civilly in an increasingly digital world and recognise that information posted on the Internet is public, permanent, and of lasting social impact.

The School District will make every reasonable effort to mitigate risks associated with digital technology usage, through student education and supervision, employee training and support, and through network filtering and monitoring. Digital citizenship is a shared responsibility between students, parents, educators, schools, and governments, and given the dynamic nature of digital technology, the School District's responsibility has limits. To that end, the following procedures are in effect.

1. ETHICAL GUIDELINES

Students may obtain access to the School District technology resources, including the internet and other online tools such as artificial intelligence (AI), and are expected to display appropriate behaviour and accountability. The use of School District technology resources is a privilege, and usage may be revoked at any time for inappropriate conduct.

As such, students must:

1.1 Review the Acceptable Use of Digital Technology policy in order to gain access to the School District technology resources and understand compliance with the policy as a condition of their access.
1.2 Use assigned devices as directed by their teachers.
1.3 Show consideration to other students when accessing digital resources.
1.4 Protect access to their individual network account under the use of a private, personal password. Ensure that their password is not shared.
1.5 Refrain from deliberately disrupting system performance or interfering with the work of other students.
1.6 Refrain from unauthorized reading, modifying, or deleting personal files owned by other users.
1.7 Not use technology to engage in or share discriminatory, obscene, profane, inflammatory, embarrassing, threatening, or disrespectful content.
1.8 Refrain from intentionally damaging equipment.

1.9 Not plagiarize the work of others or use artificial intelligence (AI) tools to cheat or plagiarize.
1.10 Be mindful of the personal information you share when using online and AI tools.
1.11 Leave devices and peripherals in their designated places.
1.12 Leave equipment/devices in good condition.
1.13 Always log off devices after finishing work and lock an unattended workstation.

2. RESPONSIBILITIES

Information and Technology Services will:

2.1 Establish and maintain sustainable service offerings which include:
- Hardware, software, and configuration standards.
- Operational strategies for hardware and software (e.g. computer installation, user accounts administration and virus protection strategies).

2.2 Provide access to School District technology resources (websites, email, etc.) to users outside of the School District.
2.3 Monitor activity on the School District technology resources and follow established processes and procedures, when necessary, to protect the integrity of the network. Actions may include revoking individual privileges or entire site privileges where it is deemed that temporary exclusion from the network is necessary to maintain the health of the network.
2.4 Adhere to the *Freedom of Information and Protection of Privacy Act*.
2.5 Provide resources and training to help govern the appropriate use of School District technology resources.
2.6 Take measures to prevent objectionable and illegal access of information. Internet access carries with it the potential to encounter information that is inappropriate for students. The Board of Education reserves the right to block any external material or content accessed through School District technology resources.
2.7 Endeavour to provide a reliable, sustainable technology environment.

School/site administrators will:

School and site administrators provide student access to School District technology resources to maximize educational opportunities. School/site administrators are responsible for the following:

2.8 Notify parents about policies governing student use of District technology resources.

2.9 Ensure that students and parents are informed of the Acceptable Use of Digital Technology policy which is included in each school's Code of Conduct prior to allowing student access to School District technology resources.

2.10 Ensure that parents/guardians are aware of the individual student's responsibility to use School District technology resources in an ethical and educational manner. Safe practices include personal safety when online and personal health and safety practices.

2.11 Ensure that students and staff are trained in the safe use of School District technology resources and that they understand the inherent risks associated with using technology.

2.12 Ensure that resources are available to help staff guide students in managing appropriate student use of digital technology.

2.13 Ensure appropriate student supervision through staff oversight, including (but not limited to) internet activity.

2.14 Ensure the equitable provision of digital access to all students.

2.15 Approve site-based technology initiatives.

2.16 Ensure that all student access to the internet, while on school property, is through School District technology resources and their School District-provisioned account.

2.17 Ensure that school-based technology activities adhere to Board of Education policies and district practices.

Teachers and Educational Assistants will:

In order to facilitate student access and to ensure the appropriate use of School District technology resources, teachers and educational assistants will:

2.18 Review and comply with the Board of Education's policy 2700 - Acceptable Use of Digital Technology.
2.19 Know the status of the students' parental consent.
2.20 Instruct students in the effective and ethical use of the internet, social networking tools, artificial intelligence (AI) tools, and other collaborative technologies.
2.21 Provide guidance to students for minimizing online risks.
2.22 Encourage parents' involvement in developing their children's digital citizenship.
2.23 Monitor student use of School District technology resources.

Students will:

Students are responsible for reviewing and complying with the Acceptable Use of Digital Technology policy which is included in each school's Code of Conduct. This provides students with the following:

- Access to the School District network
- Access to School District software solutions
- Access to the internet
- Access to the school library catalogue
- Access to electronic file storage
- Access to printing

3. SECURITY

The School District uses internet filtering and monitoring as a means of preventing access to material that is obscene, illegal, and/or harmful to minors. This filtering applies to all devices accessing the internet through School District technology resources, regardless of whether the devices are School District-assigned or personally owned. If monitoring leads to the discovery that a student has failed to follow the policy and district practices, then a fair and reasonable investigation will be carried out. As a preventative measure, the following terms must be adhered to by students:

3.1 Students are only to access real-time messaging and online chat with the permission of the teacher. Students will not reveal their personal information (such as last name, home address, email address, images, school name, phone number or anything that personally identifies themselves) while in correspondence with unknown parties.

3.2 Students are responsible for reporting any inappropriate material they receive, or any material that makes them feel uncomfortable.

3.3 Students are prohibited from viewing, sending, and accessing illegal material, or any other internet-based material that is inconsistent with the educational mission of the Rocky Mountain School District No. 6.

3.4 Students are prohibited from downloading inappropriate or illegal material.

4. PERSONALLY OWNED COMPUTING/NETWORK DEVICES (BYOD)

4.1 Where applicable, appropriate virus-checking software must be installed, updated, and made active prior to any personally owned computing device being placed on the School District's network.

4.2 Personal devices should be brought to school fully charged.

4.3 Students should avoid bringing peripheral devices, such as chargers and charging cables to school.

4.4 No device connected to the School District's network will have software that monitors, analyzes, or may cause disruption to School District technology resources.

4.5 The School District is not responsible for any device or data loss, theft, damage or other associated costs of replacement or repair as a result of a student bringing their own device to school.

4.6 School District employees will not be responsible for supporting or troubleshooting a student-owned device.

4.7 Students will take full responsibility for any personally owned device and will appropriately secure all devices when not in use.

5. DISCIPLINARY CONSEQUENCES

The School District reserves the right to monitor and inspect all activities connected to School District technology resources, including activities from personal devices. A search and investigation associated with any student's School District-provisioned computer account will be conducted if there is reasonable suspicion that the terms of this district practice have been violated. Discipline for inappropriate use may include, but is not limited to, one or more of the following:

- Parents will be contacted and provided with the opportunity to be informed of, and defend or explain student misconduct.
- Temporary confiscation of the student's personally owned device(s) by school authorities.
- Revocation of access to School District technology resources, including (but not limited to) internet access, wireless access, use of school and/or personal devices and printing;
- Disciplinary action according to applicable Board of Education policies.
- Legal action, according to applicable laws.

6. EVALUATION

Due to the dynamic nature and associated risks of digital technology, this practice will be reviewed and revised if necessary, on an annual basis.