Rocky Mountain School District #6

**DISTRICT PRACTICE 2700.1**

**EMPLOYEE ACCEPTABLE USE OF DIGITAL TECHNOLOGY**

---

**DISTRICT PRACTICE:**

In connecting employees to a variety of electronic resources, including access to the internet and connections with other users, the Board of Education recognizes the importance of providing clear guidelines surrounding digital technology usage.

The School District's technology tools, systems, and networks are intended for educational purposes, as well as for business and administrative functions directly in support of the School District's operation. The School District will ensure that employees and other users are aware of the guidelines and expectations related to technology, as stated below.

## 1. ETHICAL GUIDELINES

1.1 The use of School District technology resources is a privilege, not a right, and usage may be revoked at any time for inappropriate conduct.

## 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 students and staff outside of the School District;

2.3 Monitor activity on the School District technology resources and follow established processes and ~~procedures~~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 District technology resources.

2.7 Endeavor to provide a reliable, sustainable technology environment.

**Human Resources and/or school/site administrators will:**

2.8 Notify employees about policies governing staff use of School District technology resources.

2.9 Ensure that employees are informed of the Acceptable Use of Digital Technology policy prior to allowing staff access to School District technology resources.

2.10 Ensure that employees are aware of their individual 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 employees 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 Approve site-based technology initiatives.

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

**District employees will:**

2.16 Read and comply with:

- Policy 2700 – Acceptable Use of Digital Technology.
- District Practice 2700.1 – Employee Acceptable Use of Digital Technology.

2.17 Supervise student use of School District technology resources:

- Be familiar with District Practice 2700.2 – Student Acceptable Use of Digital Technology.

2.18 Report incidences of technology misuse to the site principal/manager.

2.19 Protect their provisioned account credentials from others and will not use other users' passwords and accounts.

2.20 Exercise good judgment and use technology for educational or School District related administrative purposes.

2.21 Respect School District property and be responsible for its use.

2.22 Be courteous and communicate online with the same level of respect as in face-to-face situations at all times.

2.23 Respect copyright and software licensing laws.

~~2.23~~2.24 Safeguard sensitive district employee and student information and be attentive to this requirement when utilizing online resources and artificial intelligence (AI) tools.

**School District employees are prohibited from:**

2.24 Attempting to gain unauthorized access to School District accounts, or to go beyond their authorized access.
2.25 Revealing their password to anyone.
2.26 Using inappropriate language in electronic correspondence.
2.27 Engaging in prejudicial or discriminatory activity.
2.28 Posting photographs and/or video images of students on any website without prior written consent from the student and/or parent/guardian.
2.29 Posting student's personal information, such as class lists, marks, and demographics, in a non-secure environment.
2.30 Copying or downloading copyrighted and/or intellectual property materials, such as movies, music, and images. Critical thinking will be required to assess the source of information when utilizing artificial intelligence (AI) tools.
2.31 Posting false or defamatory information.
2.32 Knowingly accessing illegal, discriminatory, harassing, obscene, pornographic, racist, libelous, threatening resources that are sexually explicit or promote physical violence.
2.33 Using electronic mail to send obscene, anonymous, threatening, harassing, libelous, discriminatory, or inflammatory messages.
2.34 Accessing, transmitting and/or duplicating materials, in violation of provincial and/or Canadian laws.
2.35 Using School District technology resources for commercial, political, or illegal purposes.
2.36 Vandalizing or attempting to destroy School District data and School District technology resources.
2.37 Engaging in spamming activities using School District technology resources.

## 3. SECURITY

3.1 Users must not download computer software or information that may compromise School District technology resources.
3.2 Any user identified as a security risk may be denied access to School District technology resources until further adjudication is performed.
3.3 All incidences of vandalism must be reported to the school/site administrator. Where appropriate, the School District will seek reimbursements for costs incurred.
3.4 The School District reserves the right to monitor all user activity of School District technology resources.

## 4. DISCIPLINARY CONSEQUENCES

According to Canadian common law and provincial privacy legislation, employees are afforded certain privacy rights related to their use of School District technology resources. However, a search and investigation of any user's School District-issued computer account will be conducted if there is reasonable suspicion that the terms of policy 2700 have been violated.

Allegations of unacceptable use of School District technology resources will be addressed according to established policies and practices. Discipline for inappropriate use may include, but is not limited to, one or more of the following:

- Temporary or permanent revocation of access to School District technology resources.
- Disciplinary action according to applicable Board of Education policies.
- Legal action according to applicable laws and contractual agreements.

## 5. EVALUATION

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