Administrative Procedure 600

TECHNOLOGY ACCEPTABLE USE

Background

The use of electronic devices, telecommunications, networked services and cloud services provide enhanced learning / collaboration opportunities and efficiencies and for students and staff.

Definitions

1. Technology is defined as all electronic devices, telecommunications, networked services and cloud services.

2. Acceptable use is defined as a responsibility of each user of Division or school technology to ensure that such use supports educational activities consistent with the Division's mission and goals, and complies with the information security requirements of the Division.

   The following activities do not meet acceptable use criteria:
   - Committing illegal or unethical acts, including any use of technology to plan or carry out acts of fraud, theft, harassment or vandalism, or to damage or destroy digital information or information resources.
   - Transmitting or gaining access to any material that breaks copyright or material protected by trade secret, or committing plagiarism of information.
   - Transmitting or gaining access to obscene or threatening material, written or pictorial, including but not restricted to material that contains or promotes pornography, racial supremacy or ethnic hatred or violation of human rights.
   - Using Division technology for unauthorized commercial activities by for-profit organizations.
   - Using Division technology for unauthorized product advertisement.
   - Creating or uploading unlawful material using Division owned or accessible technology..
   - Conducting activities that are wasteful of technology resources or that degrade or disrupt technology performance, including other technology accessed on the internet.
   - Sending messages that include profanity, vulgarities, or any other inappropriate language, including sexual, racial, religious or ethnic slurs, or any abusive, threatening or otherwise offensive language.
   - Revealing, without consent from the person(s) affected, any personal addresses, phone numbers or identifying information of other persons or otherwise invading their privacy.

- Breaking any confidentiality of any account or password or making them accessible to others.
- Using a school or division logo for which they have not received explicit permission from the school principal or the division executive respectively.

3. Vandalism is defined as any malicious attempt to harm, modify, or destroy hardware, software or data; theft of hardware, software or data; or unauthorized access.

4. Harassment is defined as the persistent annoyance of another user, or the interference of another user's work. Harassment includes, but is not limited to, the sending of unwanted messages.

Procedures

1. Purpose and privilege of access to Division technology.

   The purpose of providing access to Division technology is to promote educational excellence by:
   - increasing the availability of technology based resources,
   - facilitating communication, collaboration and research, and
   - supporting current educational technology standards.

   The use of Division technology is a privilege, not a right, and unacceptable use may result in cancellation of the privilege for any user, whether that user is a student, a Division staff member, Division partners or a members of the public.

   Access to technology will be provided to students, staff, partners and members of the public who sign the Division's Code of Conduct and agree to practice acceptable use, and agree to the terms and conditions established in school and Division procedures.

   Any user violating these procedures, or any applicable provincial, federal, or international laws, or posted classroom, school, or Division rules, is subject to loss of technology privileges and any other Division disciplinary options.

   The Superintendent or designate has the authority to determine what constitutes acceptable use.

   Each principal shall enforce the Division's acceptable use technology procedure.

2. Monitoring technology use and responsibility for unacceptable material access.
   The Superintendent or designate may review any information accessed or created using Division technology and may monitor technology in order to make determinations on whether specific uses are acceptable.

The Superintendent or designate may establish guidelines for the development and maintenance of school, staff, or student websites.

The Superintendent or designate may establish guidelines to protect privacy and Division technology.

In addition to such Division guidelines, all users are expected to follow guidelines as determined by Alberta Education.

Publication of any private or personal information must also comply with the Freedom of Information and Protection of Privacy Act.

It is the user's responsibility not to initiate access to unacceptable material and cease access to such material immediately upon discovery that access has been inadvertently gained to such materials.

The Division acknowledges that is impossible to completely control the content of data that a user may discover or encounter through use of the Internet; however, the Superintendent or designate and principals may authorize the application of software programs to restrict or track access to inappropriate material.

Division staff will endeavor to provide reasonable supervision of technology, although it may not be practical to provide direct supervision of each student in every circumstance in which he or she is using technology.

3. Liabilities of the Division.

   As the owner or the administrator of Division technology, Aspen View Public Schools:
   - Makes no guarantees of any kind, whether expressed or implied, for the service it is providing.
   - Will not be responsible for any damages a user suffers. This includes loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by the Division's negligence or by the user's errors or omissions.
   - Specifically denies any responsibility for the accuracy or quality of information obtained through its services and use of any information from the Internet is at the user's risk.
   - Will not be responsible for financial obligations arising from the use of Division technology.

4. Information Security.

   The Division holds users responsible to protect their passwords and keep them private to ensure the security of all Division technology.

Where a user feels that he/she can identify a security problem, he/she must notify a system administrator and not demonstrate the problem to other users.

It is unacceptable for any user to attempt to log on as either another user or as a system administrator without permission from the Superintendent or designate.

Only Division owned and approved software programs or apps may be installed or accessed using Division technology, unless otherwise authorized by the Superintendent or designate. Permission to install or access software or apps not already vetted and approved by the Division can be obtained by submitting a Privacy Impact Assessment (PIA) to the Superintendent of designate.

Vandalism of Division technology or data and/or harassment of any user or any user's information will not be tolerated.

5. School Procedures

The principal, in cooperation with school staff, shall:

- Ensure that all of the employees and authorized users at that location are familiar with and abide by the Division technology administrative procedures (AP 6XX), and complete and sign a Division Technology Code of Conduct.
- Ensure that students shall not be granted access to Division technology until they and their parents complete and sign a Division Technology Code of Conduct, Independent students and students over the age of 18 may sign agreements for themselves.
- Maintain completed and signed student Technology Code of Conduct documents in student records,
- Ensure completed and signed staff Technology Code of Conduct documents are submitted to the Division, and
- Establish procedures to ensure adequate supervision of students using Division Technology.

Students with special needs may be exempted from signing a Technology Code of Conduct at the discretion of the principal.

Where a community training program is to be conducted using Division technology, the principal may authorize such use when satisfied that security is ensured.

Reference: Section 12, 60, 61, 113, School Act
Freedom of Information and Protection of Privacy Act
Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
A.T.A. Code of Professional Conduct

Privacy Impact Assessment (PIA)
Student Technology Code of Conduct
Student Technology Code of Conduct Agreement
Staff Technology Code of Conduct
Staff Technology Code of Conduct Agreement