Administrative Procedure 140

TECHNOLOGY ACCEPTABLE USE

Beliefs

The Division encourages the use of computer technology and networks to enhance teaching and learning, and to support administrative functions.

Guidelines

1. Use of the network and the Internet must be in support of, and consistent with, the educational objectives of the Division and must conform to Board policy and administrative procedures.

2. Students and staff will be provided with individualized accounts and passwords to access computer and online services.

3. The purposeful use of computer technology and networks:
   
   3.1 All students will have access to and use technology to enhance learning across the curriculum.
   
   3.2 All staff will have access to and use technology to enhance teaching, planning, assessing, reporting, and personal/professional development.
   
   3.3 All schools and Division office departments will use appropriate technology to enhance planning, reporting, communication, financial management, and the flow of information.
   
   3.4 Services will be available to assist schools and Division office departments in formulating and implementing plans for technology.
   
   3.5 All schools and Division office departments will plan effectively for technology integration and technology change.

4. Division technology must be used in ways that are consistent with the following principles.

   4.1 Appropriate Use

   Division technology is intended for educational purposes and for business activities in the operation of schools and the Division. Personal use of electronic communication must not interfere or conflict with its use for work purposes. Division technology shall be used for purposes that are legal, ethical and moral.
4.2 Privacy and Personal Safety

Activities involving Division technology will, as much as possible, protect the privacy of personal information of all users and the personal safety of students. All users will be educated about ways that they can protect their own personal information and personal safety.

4.3 Security of Systems and Information

Individuals using Division technology shall not compromise the security and integrity of data and information stored on Division or school computer systems.

Procedures

5. Students will be given access to Division technology for educational purposes that include:

5.1 Achieving the learner outcomes of the Alberta program of studies.

5.2 Participating in learning activities selected by the teacher.

5.3 Participating in alternate Division programs.

6. Staff will be given access to Division technology for educational purposes that include:

6.1 Communication.

6.2 Information acquisition.

6.3 Information management, such as student and financial information.

6.4 Professional development and training.

6.5 Providing technology support to other users of Division technology.

7. Community volunteers and school council representatives may be given access to Division technology for educational purposes that include:

7.1 Communication.

7.2 Information acquisition.

7.3 Assisting teachers in using Division technology with students.
8. Students and staff shall adhere to appropriate use guidelines established by the Division.

9. Schools will request that students and their parents or guardians sign an appropriate use agreement that confirms their understanding of school and Division guidelines and administrative procedures.

10. All users will be responsible and accountable for their use of Division technology.

11. Students who deliberately use Division technology inappropriately will be subject to some or all of the consequences:

   11.1 Loss of computer and network privileges.

   11.2 Suspension.

   11.3 Legal action.

12. Staff who deliberately use Division technology inappropriately will be subject to disciplinary or legal action, which may include termination of employment.

13. Other users who deliberately use Division technology inappropriately will lose the privilege of using Division technology.

14. Unacceptable use of the network includes, but is not limited to:

   14.1 Using the network for any illegal activity, including violation of copyright laws.

   14.2 Using the network in ways, which violate policies, administrative procedures, and behavior standards.

   14.3 Using the network for financial or commercial gain.

   14.4 Degrading or disrupting equipment or system performance.

   14.5 Invading the privacy of other individuals by accessing and/or vandalizing their electronic data.

   14.6 Wasting technology resources, including bandwidth, file space, and printers.

   14.7 Gaining unauthorized access to resources or entities.

   14.8 Using an account owned by another user with or without his/her permission.

   14.9 Posting personal communication without the author's consent.
14.10 Any activity that could compromise an individual’s position as a representative of the Division.

15. Network Etiquette

15.1 Be polite. Do not get abusive in your communications to others.

15.2 Use appropriate language. Do not swear, use vulgarities, or other inappropriate language.

15.3 Do not engage in activities prohibited under municipal, provincial or federal law.

15.4 Do not reveal your or any other person’s personal information (e.g., home address, telephone number, passwords, etc).

15.5 Do not reveal any passwords assigned to you.

15.6 Electronic mail (e.g., e-mail) is not private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities will be reported to the authorities and will result in the loss of user privileges, and other appropriate disciplinary actions.

15.7 Use of the network and Internet in such a way that you will not disrupt the use of the network by other users.

15.8 All communications and information accessible via the Internet should be assumed to be the private property of those who put it on the network.

15.9 If you see a security problem on the network, report it to a system administrator.

16. Use and Installation of Software

16.1 Only individuals designated by a school or site administrator shall be authorized to install software on Division computer technology.

16.2 No one shall install illegal or pirated software on any computer.
17. Filters will be used to block access to inappropriate sites and the Division network. Site administrators may grant limited access to some sites for educational or business purposes. Users may, however, encounter material that is controversial, inappropriate, or unacceptable. It is the user’s responsibility not to initiate access to such material and to cease access to such material immediately. Such material must be reported to a teacher immediately, who will in turn report the matter to a system administrator.

18. The Division shall not be liable for any decision by any service provider or by the Division itself to restrict access to or to regulate access to material on the Internet. The Division does not control material on the Internet and is therefore unable to control the content of data that a user may discover or encounter through use of the Internet.

19. The Division may monitor the use of technology on a periodic basis checking for breaches of security, violations of law, or infringement of Division rules, Board policy or administrative procedures. Such monitoring may occur electronically or manually and without prior notification.

Reference: Section 12, 60, 61, School Act
Freedom of Information and Protection of Privacy Act
Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Beliefs

The Division recognizes that using social media will enable staff and schools to develop stronger relationships with key stakeholders, keep them better informed, and provide timely information.

Guidelines

1. Social media is a variety of tools and technologies used to upload and create online content like blogs, wikis, social networking, video sharing, websites, etc.

2. The social media guidelines outlined herein apply to all employees, who engage in social media whether personally or professionally, and partners who create or communicate through blogs, websites and other social media tools.

3. Employees are representatives of the Division at all times; as such employees who engage in social media shall:

   3.1 Make only positive or neutral comments about students, staff, contractors, volunteers, parents, the Division and the Board.
   3.2 Ensure that the pictures posted and statements made would not raise concern as it pertains to the employee’s role-modelling function.
   3.3 Understand that personal and professional roles become blurred by social media and affect one another.
   3.4 Make sure that confidential information about students’ remains private.
   3.5 Not post pictures of students on social media.

4. Employees shall:

   4.1 Carefully consider everything that they post or repost:
   4.2 Engage only in positive conversations online; if a conversation with a parent becomes negative or argumentative follow up with a telephone call or in person. Employees must represent the Division professionally; even in personal social media accounts. Employees must recognize when a healthy debate has turned unhealthy (e.g., insults, etc); that’s when it is time to leave the conversation.
   4.3 There is NO DELETE button; everything posted online or posted about oneself forms an individual’s digital footprint. A passive digital footprint is created when data is collected without the owner knowing, whereas active digital footprints are created when personal data is released deliberately by a user on a website or on social media. Digital footprints are a permanent, online record that includes internet searches done from home or at school.
   4.4 Employees must protect their password; someone logged in as you is contributing to your digital footprint; this could be very damaging.
5. Employees must maintain a professional relationships with students:

5.1 Students are not friends; do not add students as friends to your personal social networking sites.
5.2 Inform students that employees do not have students as friends on their personal social networking sites.
5.3 Social media can be an extremely effective communication tool when used correctly. If a social networking site is created for a class or school, ensure it is representative of the values of the Division and the professional obligations of the employee.
5.4 Teachers must be aware that not all students have access to technology at home and homework assignments that require the use of social media are not appropriate.

6. Employees must use school social media effectively:

6.1 Create content that is relevant and important; don’t overshare.
6.2 If a mistake is made, admit it and fix it; being honest online is very important in order to establish and maintain credibility.
6.3 Professional Codes of Conduct and Conditions of Employment apply; do not comment on other teachers, principals, schools, staff, the Division, or the Board.
6.4 It is unprofessional to be a member of an online group that is disrespectful to teachers, staff, the Division or the Board; employees shall remove themselves from such groups.

Reference: Teachers and Facebook - ATA Publication E-Liability - Alberta Teachers Association