140 TECHNOLOGY ACCEPTABLE USE

Background

Technology can support, enhance, and transform learning and the way we work and learn. The Division expects that technology will be used in an ethical, legal, moral, relevant, and responsible manner consistent with the beliefs and values of the Division.

The Division believes that the use of the Internet in our schools should be for educational purposes only and under the supervision of a staff, administrator, or volunteer.

A number of unacceptable uses of the Internet are described in detail within the administrative procedure to help users understand activities that are inappropriate. All Internet usage, including e-mail communications and other communications, will be logged and may be viewed by division administration and the RCMP.

The user has no reasonable expectation of privacy with the use of the Division e-mail and personal files on the Division's networks.

Definitions

Educational purposes
Includes but is not limited to classroom activities or activities of a similar nature, career development, and any activity which derives its source from an educational provision.

Commercial purposes
Includes but is not limited to the offer or provision of products or services through the CRPS network.

Communication purposes
Includes communication or contact between staff members, teachers, board members, parents, volunteers and other individuals in the education area and colleagues within the education, government and business communities.

Harassment
Is defined as persistently acting in a manner that is distressing or annoys another person.

Vandalism

Is defined as any malicious attempt to harm or destroy data, equipment, the network, or agencies or other networks that are connected to the Internet. This includes deliberately or recklessly exposing Division technology to virus infection

Parent
Is the same as defined in the Education Act.

Plagiarism
Means taking the ideas of writings of others and presenting them as if they were one's own.

User
Is an individual who uses the Division's computer technology for Internet and e-mail purposes. This includes but is not limited to all students, teachers, board employees, volunteers and parents.

Procedures

1. The Technology Acceptable Use agreement shall be reviewed with all students (K-8) at the beginning of the school year, and once upon entering high school (9-12) .

2. The Technology Acceptable Use Agreement shall be signed by all CRSD staff.

3. A Technology Acceptable Use Form (Student) will be included in the annual online student enrollment verification and will be acknowledged annually by parents. Additionally, the terms will be reviewed at the beginning of each school year with students.

4. Division technology resources (devices, networks, etc.) may not be used to:

    a. Transmit information/material that violates Canadian/Alberta legislation.

    b. Duplicate, store or transmit pornographic material (including social media).

    c. Duplicate, store or transmit threatening, abusive or obscene material.

    d. Duplicate, store or transmit copyrighted material in violation of copyright law.

    e. Threaten, intimidate, bully or spread rumours (gossip) about another individual or group or harass other users with unwanted email (spam)

    f. Use anonymous proxies to get around content filters.

5. All users of Division owned technology, including networks, shall avoid plagiarism and other violations of copyright/licensing infringement.

6. Expected behaviour for users of social media include, but is not limited to the following:

    a. All users must conduct themselves appropriately, using proper social decorum and adhering to all applicable “codes of conduct” as may apply to them (i.e.: provincial legislation, ATA Code of Conduct, School Board rules and policies).

    b. Staff will not issue personal friend or follow requests to students and will decline similar requests from students on all social media platforms.

    c. Division technology is intended for educational purposes and as such, during the school day, it is expected that use will be limited to activities related to teaching and/or learning and work-related tasks.

7. Acceptable Use
   The following sections are to assist users to more fully understand the intent and scope of this Administrative Procedure. Failure to adhere to the Division Acceptable Use Agreement may result in the user’s access being revoked by the local school administrator and/or the Division Network Administrator.

    a. Acceptable use includes:

        i. Using the computer, network equipment or other electronic communication devices for classroom activities or projects; this may include connecting to other systems and computers through the Internet.

        ii. Sending and receiving e-mail related to school activities.

        iii. Personally accepting responsibility for all web sites and other materials accessed, downloaded, uploaded, viewed and/or produced and knowing that the content is to be appropriate for school use at all times.

        iv. Understanding that system administration personnel have access to all files at all times, including e-mail.

            - These files are logged and may be viewed by Division administration and/or the RCMP.

            - The Division will cooperate fully with local, provincial or federal officials in any investigation related to any illegal activities conducted through the Division network or with Division-owned technology.

        v. Knowing that use of technology resources is a privilege – not a right.

    b. Unacceptable use includes (but is not limited to):

i. Using profanity, obscenity, or language, which may be considered offensive or abusive to another person including but not limited to the use of vulgar, obscene, rude, lewd, inflammatory, threatening, disrespectful or derogatory language.

ii. Using the Internet or other communication devices to intimidate, bully, harass or embarrass anyone; including personal attacks, prejudicial or discriminatory attacks, or posting information or pictures that could cause damage, danger or disruption of school operations.

iii. Violating copyright laws, which include copying, sharing, downloading or installing copyrighted or unlicensed material as well as copying/printing material that is considered restricted or proprietary.

iv. Giving out individual passwords or using another individual's password.

v. Reading, copying, impersonating users, or modifying another user's e-mail, social networking, chat programs or restricted files without prior consent.

vi. For students, loading or modifying software without the consent of a staff member or local school administrator.

vii. Knowingly sabotaging computer or network equipment; this includes bypassing or disabling certain operating system functions or network configurations, i.e., such as clearing the Internet or chat history or cache.

viii. Using the computers or network for any type of illegal activity or personal gain including but not limited to on-line gaming activities, objectionable offensive or pornographic material, etc.

ix. For students, using computers or the network without permission from a teacher or staff member.

8. Internet Privacy Protections and Considerations for Students

a. All Division employees have an obligation to ensure student safety and to balance this with the need for open communications when using the Internet. There are documented instances of students being inappropriately identified via the Internet and thereby becoming subjected to unhealthy situations or unwelcomed communications.

b. Division employees are expected to assist students in regard to their use of the Internet, including personal electronic devices that access the Internet. The purposes of these procedures are:

i. To inform school staff of the possible dangers of allowing students to post or publish identifying information on the Internet;

ii. To recognize that there are potential advantages of allowing students to post or publish identifying information on the Internet; and

iii. To provide a recommended set of procedures governing how student-identifying information is to be allowed in posting or publishing on the internet.

- There can be risks, as well as advantages, involved with allowing students to be identified on the Internet. Students are not to be easily identifiable from materials they might post or publish on the Internet.

- No directory information is to be posted on the web for students whose parents have returned the form asking that such information not be released.

9. Personal Safety Guidelines

a. Staff will incorporate into learning opportunities for students, all resources provided by the District Technology Committee on an ongoing basis.

b. Students will not disclose their full name or any other personal contact information for any purpose. Personal contact information includes address, telephone or school address.

c. Students will not share or post personal contact information about other people. Personal contact information includes address, telephone, school address or work address.

d. Students will not share or post privacy-revealing personal information about themselves or other people.

e. Students are not permitted, nor should they ever agree to meet someone they have only met online.

f. Students are to tell/show their teacher or another trusted school employee (an adult) about any message they receive that is inappropriate or makes them feel uncomfortable. Students are not to delete the message until instructed to do so by a staff member.

g. Pictures that are a part of student publishing are not to include identifying information.In special circumstances, with parent-signed release, identifying information can be added.

10. Portable Electronic Devices

a. Student-assigned Division portable technology devices must follow the rules of the Acceptable Use Agreement.

b. It is the student's responsibility to immediately alert school personnel if a Division-assigned device is lost, damaged, or stolen.

c. Students using personal or Division-assigned devices are subject to all Division policies and procedures, plus any local, provincial or federal laws, when using the device.

d. Students take full responsibility for electronic personal property brought to school and are to take all reasonable measures to protect against theft or damage.

e. Technology staff will not support or configure any personal electronic device.

11. Guest Wireless Network

a. The Division wireless guest network provides limited access, fixed bandwidth and is filtered for compliance.

b. Users of this network are subject to all Division policies and procedures, and any local, provincial or federal laws related to Internet use.

c. Technical support is not provided for general guest access, unless access is related to a specific educational purpose.

d. By using technology provided by the Division, guests agree to abide by the terms and conditions of this Administrative Procedure.

i. Students of the Division must sign the agreement in order to gain access to technology. Consistent with the Code of Conduct, all students are bound by the terms and conditions of this Administrative Procedure.

12. Terms and Conditions of Use

Successful operation of technology resources in the Division requires that all users regard it as a shared resource. It is important that users conduct themselves in a responsible, legal, professional, ethical, and courteous manner while using Division technology (devices and/or networks) and when communicating online using social

media tools or other technologies. All other policies, including those on harassment, equity, and proper conduct of employees and students also apply to the use of technology. Following is a list of guidelines, the violation of which could lead to suspension or termination of access privileges and may lead to further disciplinary and/or criminal proceedings.

a. System Security and Integrity

i. Hacking into a network is a criminal act. You may not violate, or attempt to violate, the security or integrity of computers, data, or network in the Division.

ii. Users are prohibited from sharing their passwords or permitting others to use their account and must log off immediately after use to ensure that others may not access their account. Users are responsible for all activity within their account and will be held accountable for any inappropriate activity.

iii. Users are not to disclose anyone else's user ID, password, network or Internet credentials.

iv. Vandalism may result in the termination of the users technology privileges.

v. In order to enable fair use of technology, system administrator(s) may set quotas for computer/network usage and usage time limits on some technologies.

vi. In order to protect the integrity of the networks and maintain efficiency, the connection of personal technology equipment such as home computers, routers, servers, wireless devices, etc. to Division networks, is not allowed without the permission and guidance of the Division Information Technology staff. Admittance as a guest on Division networks requires all users to agree to abide by this Administrative Procedure.

b. Privacy and Confidentiality

i. Use of Division technology including Internet access and email is neither private nor confidential and may be tracked.

- Use of such technology by any individual will be logged and may be reviewed by the Division without prior notice.

- In the case of misuse or suspicion of misuse of the network or services, the Division reserves the right to access any files/data on the system.

ii. The Division may block or remove files that are unacceptable or in violation of this Administrative Procedure.

iii. Parents have the right, where legally applicable, to request to see the contents of their child's data.

iv. Due to the nature of some Division approved online technologies being hosted worldwide (e.g.Google Apps), it is possible that an individual's full name, student ID, school name, email and classwork, may be stored on premises outside Canada. In such cases, privacy laws of the country hosting the data may apply. Such technologies may only be used in the manner prescribed by the Division

.

v. The Division will not disclose or post a student's personal contact information without the consent of the student's parent or of the student, if of legal age. This includes the student's address, telephone number, school address, work address, or any information that clearly identifies an individual student.

vi. The Division will not disclose an employee's personal information without the consent of the employee.

vii. Staff and students shall not post or discuss online, personal information or work-related issues including student work, without the permission of all parties involved.

viii. When using social media or other websites to enhance classroom education or conduct Division business, personal information including full names may not be posted unless authorized, and appropriate measures are to be taken to protect the privacy of individuals and content where applicable.

13. Notice of Fair Warning

a. All users of technology owned by the Division and/or those who access school/system networks (including staff, students and parents) are to understand that steps are routinely taken within the Division to mitigate the connection to or the downloading of offensive material. However, due to the dynamic nature of the Internet, there is no fail-safe way to ensure that students or staff are completely isolated from controversial, offensive or questionable content.

b. The Division and its individual schools are not responsible for the information on remote systems.

c. Furthermore, it is understood that users will change passwords periodically and are responsible for logging off local and remote systems when they are not present.

d. Users are to be aware that any discovered illegal activity carried out over the Internet may be reported to law enforcement officials for possible prosecution. Financial and legal consequences of such actions are the responsibility of the user (staff, volunteer, and student and student's parent)

Forms

Technology Acceptable Use Form (parent and student)
Technology Acceptable Use Form (staff)

Cross reference - AP 146

References

Section 31,32,33,52,53,196,197,222 Education Act
Freedom of Information and Protection of Privacy Act
Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
I.T.I.L. Standards, Alberta Education
ATA Code of Professional Conduct

History

Developed: August 2003
Amended: February 2020