Clearview Public Schools
We All Belong – We All Succeed

Administrative Procedure 140 - Computer Network Acceptable Use

Background

The use of computers, telecommunications, and networked services provides increased access to learning opportunities with the potential to improve student outcomes in their preparation for life and work. Furthermore, it provides staff, trustees, and community members with similar opportunities to enhance their contributions to the Division's mandates and functions. Teaching, learning and communication practices that utilize networks, Internet access, and other approved electronic resources are endorsed.

Procedures

1. It is the responsibility of each user of Division or school networks to ensure that such use:

    1.1. Supports educational activities and communications consistent with the Division's mission and goals; and

    1.2. Complies with the computer network security requirements of the Division. Note: The following activities include, but are not limited to, activities that do not meet acceptable use criteria:

        1.2.1. committing illegal or unethical acts, including any use of the network to plan or carry out acts of fraud, theft, harassment or vandalism, or to damage or destroy digital based information or information resources;
        1.2.2. transmitting, or gaining access to any material that breaks copyright or material protected by trade secret, or committing plagiarism of information;
        1.2.3. transmitting, or gaining access to obscene or threatening material, written or pictorial, including but not restricted to material which contains or promotes pornography, racial supremacy or ethnic hatred or violation of human rights except where authorized by school administration or teaching staff in relation to approved curricular activities;
        1.2.4. using Division networks for unauthorized commercial activities by for-profit organizations;
        1.2.5. using Division networks for unauthorized product advertisement;
        1.2.6. placing unlawful material on an electronic digital system within, or accessed by the Division network;
        1.2.7. conducting activities that are wasteful of network resources or that degrade or disrupt network performance, including other networks and systems accessed on the Internet;
        1.2.8. 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;
        1.2.9. revealing over the network, without consent from the person(s) affected, any personal addresses, phone numbers or identifying information of other persons or otherwise invading their privacy;

1.2.10. breaking any confidentiality of any account or password or making them accessible to others;
1.2.11. vandalism which is defined as any malicious attempt to harm, modify, or destroy data of another user on the wide or local area network, the Internet, or other networks. This includes, but is not limited to, the uploading or creating of things such as computer viruses, malware, keylogging etc.
1.2.12. harassment in the network context which 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 mail, unwanted messages, etc.
1.2.13. attempts to circumvent security or protection systems are prohibited. This includes, but is not limited to, VPN, Proxies, etc.

1.2.14. Signing up to any non-education site or subscription with your Clearview email. This includes but is not limited to, Snapchat, VSCO, Instagram, Tik Tok, Discord, other social media sites, or games sites.

2. Purpose and Privilege of Access to Networks

2.1. The purpose of providing access to networked services and the Internet is to promote educational excellence by:

2.1.1. increasing the availability of technology-based resources;
2.1.2. facilitating communication in support of research and education; and
2.1.3. providing staff, students, and approved community members with opportunities to develop computer literacy skills.

2.2. The use of computers, networks, Internet and information services is a privilege, not a right, and unacceptable use may result in the cancellation of that privilege for any user, whether that user is a student, a Division staff member or a community member.

2.3. The Division supports and respects each family's right to decide whether or not to allow their child to apply for access to the Division network. Ultimately, parents are responsible for setting and conveying the standards that their children are to follow when using media and information sources.

2.4. Access to Division computers, networks, internet and information services will be provided to students, staff, and community members, and users agree to practice acceptable use and agree to the terms and conditions established in school and Division procedures.

2.5. Any user violating:

2.5.1. these guidelines; or
2.5.2. any applicable provincial, federal or international laws; or
2.5.3. posted classroom, school or Division rules; is subject to loss of computer and internet privileges and any other disciplinary options, up to and including termination of employment, provided within Board policy, administrative procedures and/or the relevant legislation/regulations.

2.6. Each Principal, in consultation with the Director of Technology Services, shall have discretion at the school level in determining what is an acceptable use of the network within the policies and procedures of the Division.

2.7. The Superintendent has the authority to provide an interpretation of what constitutes acceptable use. Criteria to be used in assessing the severity of violation may include, but is not restricted to:

2.7.1. the nature of the violation;
2.7.2. whether or not students had access to the material;
2.7.3. the time of day when access occurred (i.e. was it disruptive to work/learning time);
2.7.4. frequency (i.e. one time only; frequent, and consistent over time); and
2.7.5. whether Division or personal equipment was being used.

2.8. In such matters as expulsion hearings or where appeals are made by parents or students aged sixteen (16) or over, the Board may also determine what constitutes acceptable use.

3. Monitoring Network Use and Responsibility for Unacceptable Material Access

3.1. The Superintendent may review any material on student, staff and community member accounts and files to monitor server space and/or to make determinations on whether specific uses of the network are acceptable.

3.2. The Superintendent may establish guidelines from time to time for the development and publication of school, staff, or student home pages, students' school work/projects or similar material on the Internet in order to protect the personal safety of users and the integrity of the network.

3.3. In addition to such Division procedures, all users are expected to follow guidelines for Internet publication and/or use issued by Alberta Education from time to time, and any municipal, provincial or federal legislation.

3.4. Publication of any private or personal information must comply with the *Protection of Privacy Act.*

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

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

3.7. Division staff will endeavor to provide reasonable levels of supervision of computer network access, although it may not be practical to provide direct supervision of each

student, staff member or community member in every circumstance in which he or she is using computers or networked services.

4. Liabilities of the Division

    4.1. As the owner of the computer and network equipment, the Division:

        4.1.1. makes no guarantees of any kind, whether expressed or implied, for the service it is providing;
        4.1.2. 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;
        4.1.3. 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;
        4.1.4. will not be responsible for financial obligations arising from unauthorized use.

5. Network Security

    5.1. Users are responsible to use a strong password(s) and protect their password(s) and keep them private to ensure system security, and are strongly recommended to adopt the use of 2FA/MFA.

    5.2. Where a user feels that they can identify a security problem on the network, he/she must immediately notify a technology department member and not demonstrate the problem to other users.

    5.3. It is unacceptable for any user to attempt to log on as either another user or as a system administrator without permission from authorized Division network officials.

    5.4. Only Division or school-owned software programs may be installed on Division computers and the Division network unless otherwise authorized by the Superintendent.

    5.5. Vandalism of computer or network equipment, software or file data (including theft or unauthorized entry) and/or harassment of any user or any user's file information will not be tolerated.

    5.6. All computer records, including but not limited to electronic communication related to the Division's mandate and function, may be accessed by the Superintendent.

    5.7. Users have limited privacy expectations in the contents of their files and records of their online activity while on the Division's computer network.

    5.8. Knowledge about network security is an individual responsibility, and each user should be familiar with and avoid common security risks such as spam, scams, malware, ransomware and clicking links without attempting to establish if they are safe.

6. Agreement Requirements

6.1. The Principal, in cooperation with the school staff of each school, shall:

6.1.1. ensure that information about Division network procedures and practices is provided to all students, staff and authorized users.
6.1.2. ensure that this administrative procedure is included in the student handbook provided each year to students or a current URL link to this administrative procedure on the Clearview website;
6.1.3. establish procedures to ensure adequate supervision of students using the network; and

6.2. Community members or community user groups must have permission from the Principal, in consultation with the Director of Technology Services, in order to be authorized to access and utilize the computer network.

6.3. Where a computer/network community training program is to be conducted at a Division computer terminal(s), the Director of Technology Services may authorize such use when satisfied that the network security is ensured.

6.4. Suspected abuses are to be reported to the Superintendent.

Reference: Section 31, 32, 33, 52, 53, 196, 222 Education Act
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

Effective: 2010-06-23
Amended: 2013-10-17; 2022-01-01