Pembina Hills
PUBLIC SCHOOLS

Technology Acceptable Use

AP 80-05

Procedure:

All staff and students will:

1. Keep personal information and activities (yours and others) private.
   a. Information which violates or infringes on the rights of any other person, including the right to privacy will not be published, displayed, or transmitted on the network or any computer system.
   b. Network accounts are to be used only by the authorized owner of the account for authorized purposes. The user's login password must be kept private. Do not reveal passwords, personal addresses or phone numbers of yourself or others. Users are responsible for any traffic through their account as well as any data found in their home directory on the file server. Division devices or services can be audited at any time by technology staff members for the purposes of maintaining safe and legal environments. There should be no expectation of privacy with regards to personal activities. Any confidential data or communication not related to the Division should be kept on personal devices.
   c. Users shall not intentionally seek information on, obtain copies of or modify files, other data or passwords belonging to other users or misrepresent other users on the network. Any user in possession of another user's password or access to a user's file(s) shall have their privileges suspended immediately. User accounts left logged in without a user at the station will have their account temporarily disabled by a network administrator until the user changes their password to help prevent inappropriate and unauthorized access to the network.
   d. Division administrators may choose to ban or otherwise regulate the possession of and/or use of all electronic/digital devices including but not limited to smartphones, tablets, PDA's (personal digital assistants), or any combination thereof.

2. View materials that anyone could view, and at appropriate times.
   a. It is the responsibility of each user to make good decisions as to what information is retrieved and what is done with that information. No liability will be assumed by the Division or any Division employee for any user's use or misuse of the system.
   b. The Division will provide professional development opportunities on procedures for the use of technology resources as it relates to Internet safety.
   c. Students may find material on the Internet that is considered objectionable. The use of filters and supervision while students are using the Internet does not guarantee that students will not access inappropriate materials. Students must report inappropriate access of material to a teacher or responsible staff person.
   d. Unacceptable use includes but is not limited to accessing or transmitting material that is pornographic, obscene, or sexually explicit.

3. Respect the technology resources of the Division and others and those that make sure it works right/properly.
   a. Users agree to report any observed violations to Information Technology Services immediately. If a user feels they can identify a security problem or vulnerability in the computer system, they agree to notify a staff member immediately. The user agrees not to demonstrate the problem to others.
   b. Use the network resources appropriately in such a way that you would not disrupt

the use of the network by others.

c. Use of peer2peer applications may be limited (applications that communicate directly between devices. For example: File sharing, direct video or chat).

4. Present themselves in a respectful manner in regards to technology resources.
   a. Information containing defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, intimidating, racially offensive, violent, or otherwise biased, discriminatory or illegal material will not be published, displayed, or transmitted on the network, computer system, or other device capable of instant messaging.
   b. Be polite and use appropriate language. Do not write or send abusive messages. Do not swear, use vulgarities or any other inappropriate language. Substituting symbols (i.e. **$,#,%,*,~)** in place of letters as part of such words is also inappropriate.
   c. Users of the Division web/video conferencing systems must ensure they behave in an appropriate manner at all times.
   d. Refrain from any illegal activities.

5. Respect the rights of others to have their work recognized.
   a. Computer and Internet users will review and download only information, computer software or images that are classroom related, have educational value, and are consistent with the Board's educational goals. All software materials required to meet the requirements of course curriculum will be provided by the school and any software found in a user's home directory on a file server may be removed and will be considered a breach of the Technology Acceptable Use Agreement.
   b. Unacceptable use includes the use of unlicensed software and/or use of licensed software in excess of licensing arrangements.

6. Understand that use of technology resources is a privilege and must be treated as such.
   a. User accounts will be terminated when the user is no longer affiliated with that site. User accounts will also not be fully activated until a copy of the Technology Acceptable Use Agreement has been signed, placed on file, and Information Technology Services has been advised.
   b. Electronic messaging is NOT guaranteed to be private; network storage areas are Division property and may be reviewed by appropriate staff. Inappropriate messages can result in suspension of privileges and other disciplinary actions.
   c. Although the Division does not make a practice of monitoring the use of electronic messaging, it reserves the right to audit and retrieve content for legitimate reasons such as finding lost messages, investigating wrongful acts or recovering from system failure.
   d. Unacceptable use of technology resources for personal gain could include and is not limited to:
      i. Private financial or commercial gain
      ii. Promotion of political activity
      iii. Accessing or transmitting material that is disparaging of others such that it may create a hostile work or educational environmental based on race, sex, national origin, sexual orientation, age, disability, religion or political beliefs
      iv. Accessing improper confidential information concerning students or other employees
      v. Sending or forwarding "chain mail" messages or spam
      vi. Any unlawful or unethical purpose

7. Respect Division property, including hardware and software, as well as the property of others.
   a. School equipment is to be used for legal purposes only. No illegal activity is

permitted. Users are subject to all provincial and federal laws and understand that illegal activities may be reported to law enforcement authorities. Any unethical use of technology resources will result in immediate suspension of network access privileges and/or Internet access privileges. All suspensions will be evaluated by Division administration, and re-instatement of privileges will be at their sole discretion. Unacceptable use includes:

i. Using the network for any illegal activity, including violation of copyright or other laws. This includes download of music, video or other files that are protected by copyright law.
ii. Using the network in ways that violate school policies, Division administrative procedures, and behavior standards.
iii. Invading the privacy of other individuals by accessing and/or vandalizing their computerized data.
iv. Gaining unauthorized access to resources or entities.
v. Using an account owned by another user with or without their permission.
vi. Sending, receiving, viewing or downloading illegal material via the computer system.
vii. Posting material created by another without their consent.
viii. Submitting, posting, publishing or displaying any obscene, profane, threatening, illegal or other inappropriate material.

b. Users will not obtain, install, store or use software obtained in violation of the appropriate vendor's license agreement (i.e. activities commonly called "piracy"). This includes appropriate use of site licensed software, network use software, concurrent use software, and single license software.
c. Handle computer equipment with care and respect. Users will not physically damage or remove any computer related hardware.
d. The user agrees not to tamper with or attempt to illegally "hack" or intentionally damage any computer resources. This may include changing the control panels, colors, features, and formats of any operating system or application software.
e. Any malicious attempt to harm or destroy data of another user will not be tolerated.
f. Any questionable action will result in cancellation of privileges.
g. If obvious damage to equipment is not reported when found, it will be deemed the responsibility of the user who failed to report it.
h. Plagiarism or the copying of material and representing it as your own work is also prohibited.

8. Recognize a prohibition on any type of bullying activity. Within the context of this document that refers specifically to cyber-bullying including, but not limited to, the items listed below for the use of computer based tools to:
   a. Gossip about or embarrass another
   b. Spread rumors
   c. Set up another to look foolish or take blame
   d. Publically humiliate another
   e. Manipulation of the social order to cause rejection from a group
   f. Exclusion from a group
   g. Use of ethnic slurs, racism, and homophobia
   h. Threats of withdrawal of friendship
   i. Negative comments about another person's appearance, clothing or other personal effects
   j. Distribute an intimate image of another person without consent knowing that the person depicted in the image did not consent to the distribution, or being reckless as to whether or not that person consented to the distribution

Consequences of Unacceptable Use

Non-compliance with this user's agreement will result in the suspension or termination of computer privileges. Any violation of the Technology Use Agreement will result in disciplinary action. Such consequences may be any combination of the following depending on the severity of violation and on the chronic nature of violations:

Students

1. conference
2. detention
3. termination of computer privileges, or Internet access
4. suspension at the school level and expulsion consistent with school and Division policy on student behavior
5. referral to civil law enforcement agencies, and/or fines that would include down time and cost for repairs

Staff

As per the applicable Collective Agreement or Non-Union Staff Employment Conditions Handbook.

Reference

School Act, section 1(1.1)
Policy 19 Welcoming, Caring, Respectful, and Safe Environments
Policy 23 Information and Technology
AP 80-01 Digital Citizenship
AP 80-10 Information Security
Form 8-01 Technology Acceptable Use Agreement for K-12 students
Form 8-02 Technology Acceptable Use Agreement for Staff and Trustees