

SCHOOL DISTRICT NO. 92 (NISGA'A)

Regulation Subject: Acceptable Use of Information Technology Resources (AUP)

Dated Passed: 99.06.08

Date Amended: September 9, 2008

Description:

Acceptable Use of Information Technology Resources (AUP)

Policy No. 312 – R

Definitions:

- “Information Technology Resources” include all computing equipment and computer networking devices and services. It includes any electronic device that exchanges information with a computer including, but not limited to District issued laptop and desktop computers and peripherals, the District Network includes wired and wireless communication devices that connect computers to each other and to the Internet.
- A “network account” is a means to control access to resources found within the network. It includes a network ID and a password.
- “Personal Internet Services” include social networking sites, hotmail accounts, personal blogs and other services not under the control of the School District.
- “Post” means to make information available on the Internet. This would include a user profile, a discussion board, and a blog. It would also include a “link” or a reference to another web resource.
- A “user” is a person who uses a computer to connect to a network device.
- A “personal device” or account is any equipment not owned by the School District.
- “Sensitive Information” personal, confidential or protected information whose release is unauthorized i.e. information that is reasonable likely to fall under the Freedom of Information and Protection of Privacy Act.
- “Offensive material” includes, but is not limited to, pornographic images and content, hate literature or any material that contravenes the BC Human Rights Act.

Procedures

- Prior to being allowed access to the District Network users must apply for an account and in so doing acknowledge the purposes, benefits and risks associated with the use of this resource. All users of the District Network must read and agree to abide by the Acceptable Use Policy as a condition of receiving and maintaining a network account. Access to the network is only made available so long as the user complies with the Acceptable Use Policy. This Agreement expires each August and must be renewed annually.
- The Principal or designate shall ensure that all students who use information technology, and their parents, agree to the Acceptable Use Policy as per Form 312 - F. If the situation requires it, a principal or teacher may agree to give access to a student on behalf of a parent. District administration, or designate shall create and supervise staff accounts.
- The District Technology Department working on behalf of the Superintendent of Schools will determine what is deemed inappropriate use as per the acceptable use policy, and report any infraction to the appropriate supervisor for action.

Privilege of Access and Privacy

- The use of the District computer network resources is a privilege, not a right. Inappropriate use may result in the loss of this privilege and, depending on the nature of the offence, further action may occur including, but not limited to, notification of the RCMP.
- The Technology Department may set limits for the use of resources such as disk space and printing.
- No student shall have access to the school computer network unless specifically authorized by a principal, teacher or other designated staff members.
- Authorized users are prohibited from sharing their passwords with any other user, or permitting others to use their access accounts. Account holders are responsible for all activity within their account. Accounts are provided free of charge but remain the property of the School District.
- Whenever possible users are to use School District accounts for email and other services. Personal Internet Services may be a security threat to the District Network and other users. As a result the District reserves the right to block access to Personal Internet Services, or any other service that is deemed a security hazard.
- Personal devices are not allowed on the District Network except when inspected and approved by the District Technology Department. Once approved the owner makes them subject to this policy as a condition of being permitted to join the network.
- Computer equipment may be issued into the care of individuals within the District. Equipment so issued may be used at the discretion of the user, within the limits of this policy, but remains the property of the School District and may be withdrawn or examined at any time by the District Technology Department or the Superintendent of Schools.
- Students may take computers out of the school only by permission of a classroom teacher or principal.

- District technology staff will regularly examine District network accounts from time to time, and without notice to the account holder, to ensure compliance with this policy. Monthly reports will be made to the Superintendent of Schools.
- District Technology staff will maintain privacy and confidentiality of sensitive data if data is to be examined and may not disclose the contents of any account to any other recipient unless required to do so by law or by the policies of the School District.
- The Technology Department may suspend access specific web sites or remove locally posted messages that are deemed unacceptable.

Acceptable Use

- Use is acceptable when it is legal, ethical and upholds the goals and professional standards of the School District and the BC College of Teachers.
- Use is acceptable when it is consistent with the goals of the School District, and when it respects the rights of other users and considers the impact of their conduct on others.

Unacceptable use includes but is not limited to

- Any message that does not meet professional standards of language and tone
- Use during business hours, for a purpose that does not pertain to the employee's duties.
- Any offensive material content that is defamatory, maliciously inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially or otherwise offensive, or advocates illegal activity, or is in itself illegal
- Any content that could be understood has harassment or cyber-bullying.
- The distribution of personal or confidential information
- The access, duplication, storage or transmission of pornographic images and texts
- Use that may lead to personal financial gain or may be considered of a commercial nature
- Gambling
- Use that is intended to obscure the origin or content or any message under an assumed computer network address
- Use that provides access or distributes unlicensed software or documentation.
- Use that initiates or distributes chain letters, advertising or unauthorized solicitations
- Use that provides access electronic systems or information inappropriately or without authorization
- Use that vandalizes network resources

- Use intended to promote union political interests
- Use that over-utilizes network-intensive resources such as network games, frequently refreshing chat rooms or Internet radio
- Use that violates or attempts to violate, the security of the system or attempt to subvert other systems
- That deliberately or recklessly exposes systems to computer infections.
- Or that contravenes any other laws or regulations
- Makes excessive personal use of District resources such as bandwidth, disk storage space or paper.

Shared Content and Social Networking

- Use of personal Internet services is subject to the following restrictions:
- Users under the age of 19 must post content within the rules and restrictions put in place by a school or teacher, or in the absence of such rules, have a teacher or administrator review any content posted.
- Users may not post or send any personal information that may be damaging, threatening or dangerous to themselves or to others.
- Users may not post content that may be regarded as intimate or sexually suggestive.
- Instant messaging may only occur among individuals with whom users are already acquainted.
- Open and unregulated chat rooms are not permitted for minors without direct supervision.
- Nothing shall be posted that could be taken as a direct threat against another person.
- No post shall advocate for violation of any laws or school rules.

Teachers and administrators are responsible for reporting any student violations of the Acceptable Use Policy and must immediately ask students to withdraw from any community or social network that may pose a risk to them.

Sanctions

Users who fail to comply with the District Acceptable use Policy will face limitation or removal of account privileges. Serious or persistent violations may result in expulsion from school or termination of employment.



**School District 92 (Nisga'a)
Acceptable Use Policy Registration Form**

Please read the accompanying Policy (four pages) and sign this completed form to indicate your acceptance of the terms. Persons under the age of majority must have this form signed by a parent or guardian in the appropriate line.

**NOTE: INCOMPLETE FORMS WILL NOT BE PROCESSED.
PLEASE USE BLOCK LETTERING FOR CLARITY.**

Name: _____

School/Site Name: _____

Applicant is

- A student in Grade _____
- A Teacher
- An Administrator (or other exempt staff)
- Support staff
- Community Access participant
- Guest or temporary contractor

AUP Revision Jan. 5, 2010
I have read the Acceptable Use Policy and agree to abide by the rules therein.

Applicant Signature: _____

Parent/Guardian Consent: I have read the District's Acceptable Use Policy and agree to the rules therein. I am aware that although the District has taken reasonable steps to ensure that access to Internet content is supervised and monitored, my child may be exposed to inappropriate material on the Internet due to daily use of the District's systems. I am also aware that my child may face disciplinary action as laid out in the AUP and in accordance with the District Policy Manual, if caught intentionally violating the terms of this AUP.

I hereby give permission for my child to receive access and certify that the information in this Application is correct.

Please print name and relationship to Applicant

Signature of Parent/Guardian

Today's Date: _____

DO NOT WRITE IN THIS SECTION- ADMINISTRATIVE USE ONLY

Hire Date: _____ Termination Date: _____

Employee #: _____

Date Access Established: _____

Assigned User ID: _____

Assigned Password: _____