Sahtu Divisional Education Council

Acceptable use of Technology Policy

The Sahtu DEC is pleased to be able to offer our students, staff, trustees, and guests access to computer technology, including access to the Internet, email, locally installed educational software, certain online services, and the GNWT information technology network. We feel that access to the tools and resources of a world-wide network and understanding when and how these tools are appropriately and effectively used are imperative in each student's education.

The school's information technology resources, including email and Internet access, are provided for educational purposes. Acceptable activities include communication, record keeping, learning activities and research. If you have any doubt about whether a contemplated activity is acceptable, consult with your immediate teacher or supervisor, to help decide if a use is appropriate.

The Sahtu DEC has the right to place reasonable restrictions on the type and quantity of material trustees, staff, and students can access or distribute through the system. Trustees, staff, and students are expected to be responsible for their behaviour on education facility computers, mobile devices, email, and on the Internet. Social media—such as Facebook, wiki sites, blogs, Twitter, etc.—provides educators and individuals with powerful tools to connect to one another in their community and around the world, but it also presents potential risk. Unfortunately, some communications and materials accessible through the Internet may contain items that are illegal, defamatory or potentially offensive. Access to the Internet is provided to those who agree to act in a considerate and responsible manner.

Adherence to and the signing of the Acceptable Use Guidelines is required by all trustees, staff and students on an annual basis. The agreements are based on the current grade level of the student and their participation in instruction on appropriate use of technology and digital citizenship. Users will not damage computers, computer systems, or computer networks and will follow the rules set forth in respective laws and government, education authority and school conduct and disciplinary codes.

The Sahtu Divisional Education Council encourage the use of technology for staff and students in some classrooms. Personal use of devices in each school is at the discretion of the DEA, Principal and Classroom Teacher and subject to local policy.

The Sahtu Divisional Education Council is unable to restrict network access to Cellular Networks, however, the Principal is authorized to restrict use and access to Cell Phones in the school and classroom. This may be result in these devices being locked in a secure location during classroom hours. Students may retrieve messages during non-classroom times.

The district reserves the right to determine which uses constitute acceptable use and to limit access to such uses. The district also reserves the right to limit the time of access and availability of services and devices.

Violations of these rules may result in disciplinary action, including but not limited to, the loss of a user's privileges to use the Sahtu Divisional Education Council's information technology resources, suspension or expulsion, and possible legal action depending on the degree and the severity of the violation.

REGULATIONS

1) Guidelines for Trustees, Administration, and Staff

a) In addition to the Government of the Northwest Territories Policy entitled, *Informatics Policy Committee - Internet Use* and *SDEC Electronic Communications Guidelines*, trustees and employees of the Council and its DEAs and schools must also comply with the terms and conditions of these policies and its regulations.

b) Education facility managers (e.g., superintendent and school principals) will be responsible for ensuring the staff of their respective facilities have read, understand, and are in compliance with the *Computer Acceptable Use Guidelines* and this policy.

c) The school principal will be responsible for ensuring all students and their parent/guardian have read the *Computer Acceptable Use Guidelines* and signed and returned the waiver prior to student use of the school computers.

d) The principal will also ensure students receive instruction as to the purpose and content of the *Computer Acceptable Use Guidelines* and the potential consequences associated with misuse.

e) Education facility managers shall develop procedures and expectations to help guide schools and staff in promoting proper behaviours and practices in regards to the use of computers and social media by staff and students.

f) Principals will inform the superintendent, who will in turn inform *GNWT Insurance and Risk Management*, of any and all new websites implemented, inclusive of:
   i) the web address of each site,
   ii) the purpose of the site
   iii) the rules for posting to the site (rules must be displayed on the site)
   iv) who is the contact/moderator, and
   v) what kind of moderating there is

g) Education facility managers are owners and therefore ultimately responsible for the maintenance and content of any website, social media portal or digital communications service they choose to implement. Education facility managers have a right and responsibility to:
   i) police their digital media platforms and delete or remove any communications or materials deemed damaging to the Council, its DEAs, schools, trustees, staff or students, and
   ii) hold students and staff accountable for actions on these sites that negatively impact the Council, its schools, staff or students.

h) Education authority (Council and DEA) chairpersons are empowered to hold trustees accountable for actions that negatively impact the Council, its DEAs, schools, trustees, staff or students.

2) Guidelines for Parents

a) Prior to access being granted to a student, the parent or guardian will read, accept and sign a contract agreeing to rules for acceptable behaviour on the school computer systems, network, audio/visual equipment (for example cameras and video recorders) and on the Internet (including but not limited to web sites, email, text messaging, chat rooms.)

b) Parents are also responsible for educating their children as to the purpose and content of the *Computer Acceptable Use Guidelines* and the potential consequences associated with misuse of school computers, email and Internet.

3) Guidelines for Students

a) Prior to access being granted, students and/or their parents/guardians, will read, accept and sign a contract agreeing to rules for acceptable behaviour on the school computer systems, network, audio/visual equipment (for example cameras and video recorders) and on the Internet (including but not limited to web sites, email, text messaging, chat rooms.)

b) It is expected that students will follow any additional instructions in regard to material or web sites that parents/guardians think would be inappropriate for their children to access.

4) Unacceptable Uses for All Users

The following uses of the Council computer systems are considered unacceptable by any users in the education facilities of the Sahtu Divisional Education Council.

a) Personal Safety and Personal Privacy

Trustees, staff and students will not post personal information using education facility computers. Personal information includes, but is not limited to, pictures of students or families, home address and telephone numbers. Staff and students will promptly disclose to a supervisor any message they receive that is inappropriate or makes them feel uncomfortable. Posting private information about another person is strictly prohibited.

b) **Illegal Activities**

Trustees, staff and students will not use the computer system to engage in any illegal act. They will not attempt to gain unauthorized access to the education facility computer systems or to any other computer system or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. Deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means are prohibited.

c) **System Security**

Technology shall only be used by the person(s) authorized to do so. Staff and students are responsible for their individual accounts (email, network and other) and must take all reasonable precautions to prevent others from being able to access these accounts. Under no conditions should passwords or account information be provided to another person. A supervisor will be notified immediately when a possible security problem is identified. Trustees, staff and students will avoid the spread of computer viruses by not downloading or installing unauthorized software onto education facility computers.

d) **Inappropriate Language and Cyberbullying**

Trustees, staff and students will not use obscene, profane, vulgar, rude, threatening, or disrespectful language. Engaging in personal attacks (for example, name calling, harassing, threatening, bullying, excluding or insulting another person) or posting information that could cause damage to someone's character is not permitted. Direction or requests to remove derogatory posts and to refrain from posting further belittling messages must be respected.

e) **Privacy**

Trustees, staff and students should not expect that data files and communications will be private. All GNWT and SDEC hardware and software is monitored, and the employer can access anyone's computer, mobile device, work files, Internet/network activity, email accounts and texts. Users should be aware that information transmitted or received is considered a government record and is subject to requests for information under the *Access to Information and Protection of Privacy Act* (ATIPP). Further, computer files and network storage areas may not always be secure. In addition to the possibility of system security being compromised, online and system activity may also be monitored to ensure acceptable use and to maintain system integrity. Contributors do so at their own risk and take personal responsibility for their comments or other information they choose to provide.

f) **Respecting Resource Limits**

Computer and network services are shared resources and must be used in moderation, and with consideration of others. The computer systems are only for educational and administrative activities. Trustees, staff and students will not send chain letters or engage in "spamming" (sending an annoying or unnecessary message to a large number of people). Excessive use and "chatting" are discouraged. Users are required to remain within allocated disk space and delete email or other material that takes up excessive space.

g) **Plagiarism & Copyright**

Trustees, staff and students will respect the rights of copyright owners and will not plagiarize works found on the Internet.

h) **Inappropriate Access to Material**

Trustees, staff and students will not send, display or post offensive or inappropriate messages, material, videos or pictures. Education facility computer systems will not be used to access material that is designated for adults only, is profane or obscene, that advocates illegal or dangerous acts, or that advocates violence or discrimination towards other people. When inappropriate sites or information is identified, a supervisor will be informed immediately.

5) Limitation of Liability

The Council recognizes that the dynamic nature of on-line information makes total regulation and control impossible. The Council, District Education Authorities, administration and staff make no guarantees that the functions or the services provided by or through the computer system will be error-free. The Council and staff will not be responsible for damage or suffering, including but not limited to, loss of data or interruptions of service. The Council is also not responsible for the accuracy or quality of the information obtained through or stored on the system. The Council will not be responsible for financial obligations arising through the unauthorized use of the system.

By signing my name below, I certify that I have read the above information. Any questions concerning this policy have been discussed. My signature also certifies my understanding of, and agreement with the above policy. A photocopy of this document is as valid as the original. You may receive a copy of this document upon request.

_____ _____

Signature Date