Commission scolaire francophone du Yukon

ADM- 05

CSFY
YAEP
YEU

Directive: Use of Electronic Communication Systems

Category: Administrative Management

PREAMBLE

The principal objective of this directive is to regulate the use of various electronic communication systems, both with regard to existing equipment as well as any equipment that may be acquired in the future. One goal of this directive is to ensure the secure use of the various systems so that access to confidential information held by the CSFY is limited to those with access rights.

This directive also allows CSFY staff members to use various electronic systems for personal reasons within a strictly defined framework. Finally, this directive prohibits use of electronic systems in certain instances where it would be incompatible with the CSFY's mission or contrary to the legislation in place.

The Yukon's *Education Act*, the *Canadian Constitution*, Canadian regulations, the Yukon Government's computer use guidelines, and CSFY directives govern how information shall be handled.

DIRECTIVE STATEMENT

The purpose of this directive is to establish the CSFY's rules regarding use of its electronic systems, including but not limited to:

- Email;
- Telephones;
- Voicemail;
- Fax;
- Computers and any equipment connected to them, such as a BlackBerry;
- The internet network;
- The intranet network;
- Physical or electronic files;
- The use of information stored, communicated or processed by any of these systems.

All employees and other persons who use or have access to CSFY electronic systems (trustees, parents, students, etc.) agree to abide by the rules established in the present directive.

OBJECTIVES

- Ensure that CSFY electronic systems are used in a secure manner.
- Prevent any inappropriate use of CSFY electronic systems.
- Regulate the use of CSFY electronic systems.
- Encourage compliance with the rules governing confidentiality of information.

DEFINITIONS

- CSFY: Commission scolaire francophone du Yukon (Yukon Francophone School Board).

- Discussion forum or discussion group: a group of people who use the internet or intranet network to exchange real-time or non-real-time comments about a common subject.

- Download: the transfer of stored data or programs between a remote and a local computer over an electronic network.

- Electronic information: information in a textual, symbolic, audio or visual format which can only be accessed, stored, processed or communicated by means of information technology.

- Email: a message sent using an electronic network.

- Employee: any person employed by the CSFY or its schools who is appointed and paid, either by the CSFY or another entity.

- Encrypt: transformation of information into a cryptogram in order to render it unintelligible to any unauthorized person, thus ensuring its confidentiality.

- Information technology: all hardware, software and services used to collect, process and transmit information.

- Internet or internet network: a worldwide information network made up of a number of national, regional, and private networks which are linked by a TCP-IP communication protocol and which work together to offer a single interface to its users.

- Internet site: the place where an internet host is located and which is identified by an internet address.

- Intranet or intranet network: a private information network which uses some or all of the communication protocols and technologies of the internet network.

- Software: a set of programs designed to perform a particular task on a computer.

- Supplier: a physical person or legal entity authorized to do business and enter into a contract with a public body for the delivery of goods or the provision of services.

- User: any employee or other person (trustee, parent, student, etc.) who uses or has access to the electronic systems.

TERMS AND CONDITIONS

1. Ownership

1.1 The CSFY shall own any information or message that is created, sent, received, stored or accessible through its electronic systems as part of a user's duties. The CSFY has a limited right to audit and/or destroy any information or message that does not comply with the present directive.

2. Use of electronic systems and prohibited activities

2.1 Users shall have access to the CSFY electronic systems to carry out their duties. Personal use is only permitted as follows: use of the internet network outside of work hours is permitted as per the conditions outlined in this directive and with authorization from an immediate superior.

2.2 The CSFY reserves the right to withdraw or limit this privilege according to network requirements. For students, use of the internet network is permitted according to the regulations established by each facility and shall also comply with the provisions of this directive.

2.3 No costs shall be incurred by using CSFY resources.

3. Restrictions on message content

3.1 All communication occurring through the CSFY electronic systems shall not be defamatory, offensive, harassing, derogatory or inflammatory in nature and, without limiting the generality of the foregoing, shall not contain images or comments of a sexual nature, racial slurs, or any other image or comment based on age, race, colour, gender, pregnancy, sexual orientation, marital status, religion, political beliefs, language, ethnic or national origins, social conditions, or disabilities.

4. Prohibited activities

4.1 Users of the CSFY electronic systems shall not use the electronic systems in a manner which compromises the reputation of the CSFY. This includes, but is not limited to: using an illegal copy of software; trying to hack into other computers; possessing, distributing, viewing or sharing pornographic, obscene or hateful material; sending messages that could be considered as discriminatory or as harassment; or, engaging in any illegal activity.

4.2 Users shall not use CSFY electronic systems to: create or distribute chain letters unconnected to CSFY activities; express opinions for political purposes or promoting religious propaganda, where these opinions appear to come from the CSFY; carry out any solicitation unconnected to CSFY activities; send out any advertising unconnected to CSFY activities; send any messages related to union activities (subject to a specific agreement or as provided for in the terms of the collective agreements); participate in any gambling or betting; sign up for any mailing lists not related to CSFY activities; post any information, opinions or comments in discussion groups or on electronic billboards without prior authorization; work on the black market; illegally download, transmit or distribute any patented, trademarked or copyright-protected materials; download, transmit or distribute any confidential or private information or documents without the prior authorization of the CSFY or any other required consent; gain unauthorized access to computers or other systems; damage, alter or interfere with these computers or systems in any way; use the user ID or password of another user, or divulge any user ID or password, including the user's own, unless duly authorized; allow unauthorized access to or use of the CSFY electronic systems by a third party (including allowing unauthorized access to confidential information) or otherwise compromise the security of the electronic systems or use the electronic systems on behalf of a third party; open without authorization any email that is not addressed to the user or access another user's voicemail; send anonymous messages; create telecommunication links unless duly authorized.

5. No guarantee of confidentiality

5.1 Communications on electronic systems are not private, and their security cannot be guaranteed. Passwords and user IDs are issued in order to protect CSFY confidential information from third party access and not in order to ensure confidential treatment of staff messages. When using the internet network, employees must remember that the sites they visit may be monitored and recorded.

5.2 Users must assume that any communication – whether personal or not – that they create, send, receive or store on CSFY electronic systems may be read or heard by someone other than its intended recipient.

5.3 In order to ensure that CSFY has continual access to the information contained in its electronic systems, employees must not use personal software or any software that is not supported by the CSFY to encrypt their email, their voicemail or any other information stored on or transmitted by CSFY electronic systems without the prior consent of the CSFY.

6. The CSFY's right to monitor messages

6.1 The CSFY reserves the right to monitor, access, retrieve, read and disclose communications in certain circumstances, when:

6.1.1 It is within the rights and best interests of the CSFY to do so;

6.1.2 The CSFY has reasonable grounds to believe that a user is behaving or is about to behave in an inappropriate manner in relation to CSFY electronic systems;

6.1.3 The CSFY must access message content in order to obtain information that is otherwise unavailable;

6.1.4 The CSFY is required to do so by law or by court order;

6.1.5 The CSFY reasonably believes that a user has committed or is about to commit an act which may negatively impact the CSFY, whether directly or indirectly;

6.1.6 A user is unavailable due to death, illness or vacation, or is no longer employed with the CSFY;

6.1.7 A user has left the CSFY, as the CSFY reserves the right to retain a user's email for an appropriate period of time following the user's departure in order to ensure that any important communications can be forwarded to the CSFY.

7. Protection of information

7.1 Messages can easily be intercepted on the Internet. Confidential information belonging to or entrusted to the CSFY shall not be transferred over the Internet, by email or by any other means of electronic communication without using the highest level of security possible. Encryption shall be used for the Internet and email, and alternative measures used for other electronic systems.

7.2 Confidential information shall not be provided to CSFY employees without access rights or third parties unless specially authorized by the Executive Director, and then only if the third party signs a non-disclosure agreement approved by CSFY legal counsel. Users shall promptly dispose of any message that they do not wish to keep. It is the responsibility of the CSFY to destroy archived electronic documents once their retention period has expired. Similarly, upon a user's departure, the CSFY is responsible for destroying any confidential document that has not been physically removed from the computer's hard drive.

8. File archives

8.1 Just as with documents created, received and physically filed by a user, each user is responsible for ensuring that any document received in an electronic format which is required to be conserved is saved according to the CSFY file archive regulations. Messages that do not need to be saved shall be disposed of according to these same regulations.

9. Viruses and tampering

9.1 Any file downloaded from the Internet and any removable media storage must be scanned with antivirus software before use. Deliberately introducing a virus, attempting to penetrate security systems or unlawfully tampering with the CSFY's electronic systems are expressly prohibited. Users shall not deactivate the security systems in place or try to circumvent the security measures in place. Users must immediately report the existence of any virus, any tampering or any other violation to their immediate supervisor, who will follow up with the network administrator as required.

10. CSFY purchases

10.1 The CSFY purchasing directive applies to all purchases conducted through the electronic systems of the CSFY and its schools.

11. Acceptance of terms

11.1 All users agree to abide by the terms of the present directive in the manner prescribed by the facility or administrative department.

12. Roles and responsibilities

12.1 The Executive Director: shall ensure compliance with the present directive; shall ensure that electronic system access privileges are suspended as required; and, shall reserve the right to hire, if necessary, another authorized party to conduct suitable monitoring of the electronic systems.

12.2 The Executive Director: shall be responsible for any relevant documents and for compliance with the laws and regulations relating to enforcing this directive; shall oversee the protection of information and its "corporate" dissemination, as required; and, shall authorize monitoring requests.

12.3 Human resources (HR) managers: shall, in collaboration with the Executive Director, follow up on any required administrative and/or disciplinary measures to be taken in accordance with the collective agreements and administrative directives in place.

12.4 Information technology (IT) services: acts on behalf of the information network administrator and, upon request, may suspend access privileges to electronic systems; may perform monitoring upon specific request from the Executive Director as provided for in this section; shall issue virus alerts when necessary; and, shall ensure the electronic systems that they are responsible for are kept up-to-date and operating in a secure manner.

12.5 School principals: shall ensure that all employees and users are aware of the present directive; shall ensure that the electronic systems they are responsible for are operating in a secure manner; shall ensure compliance with the terms and conditions of the present directive; shall ensure that electronic system access privileges are suspended when necessary; and, shall ensure that HR managers and the Executive Director are informed when administrative and/or disciplinary action is required.

12.6 Users: shall provide to their immediate supervisor, in confidence, any codes or passwords necessary to access the systems that they use, when required; failing that, IT services will supply this information when requested by a user's immediate supervisor (when it comes to students working on school electronic systems, the immediate supervisor is the teacher of the group); and, shall agree to the rules outlined in the directive regarding use of electronic systems.

13. Contravention or violation of the present directive

13.1 Any violation of this directive, including breaching any confidentiality or security regulations, may result in suspension of CSFY electronic system access privileges. Violations may also result in disciplinary action, reimbursement of expenses, or termination of employment, where appropriate and in compliance with the collective agreements, laws, policies and directives in place.