CAMPBELL RIVER School District 72

Operational Procedure 140

TECHNOLOGY AND ACCEPTABLE USE GUIDELINES

Background

The district offers access to a variety of information systems for staff, student, and limited guest use. These information systems are intended for educational and/or research purposes and for conducting valid district business. The district also recognizes that personal devices may enrich learning and support instruction.

The purpose of this operational procedure is to fulfill the district's legal responsibility in ensuring compliance with provincial and federal mandated regulations.

Definitions

Computer System or Information System	Means a district computer or device connected to district systems and all peripherals (software and hardware) attached to the system. This also includes networks and wireless networks, electronic and fibre optic systems, digital cameras, cell phones, video equipment, email and voice mail, data, and access to the Internet.
System Administrator	Is a person designated by the district to manage an information system. The director of information technology is the primary system administrator for School District 72 and is responsible for the overall functioning, security and administration of the network. Under the direction of the director of information technology, IT technicians are directed to perform system administrator duties.
Authorized	Means approved by the district's primary system administrator.
Personal Devices	Includes, but is not limited to personally purchased; smartphones, tablet computers, laptops/ netbooks. Devices whose intended purpose is for gaming are not allowed.

Procedures

1. Access to the district's information systems, including Internet resources is a privilege, not a right, and will be available only so long as the user complies with board policies, operational procedures, and local, provincial, and federal laws.

2. Users must conduct themselves in a courteous, ethical, and responsible manner while using these systems. All board policies and operational procedures, including those on harassment, equity, and proper conduct of employees and students apply to the use of information systems.

3. All content created using the district's network or email system will be presumed to be the property of the school district unless otherwise agreed with the school district in writing.

4. Employees are only permitted to use their district email account (firstname.lastname@sd72.bc.ca) to conduct district business. Staff should have a personal email account for personal (non-school district related) business and correspondence. Personal email addresses are not to be used to send district communications to/from any staff member.

5. User Privacy and Confidentiality

5.1 Users do not have a personal privacy right in their actions or in any content created, received, stored in, or sent from the school district network or email system.

5.2 Use of district information systems including the Internet, by any individual, may be monitored or reviewed by district system administrator(s) and/or Provincial Learning Network system administrators without prior notice.

5.3 The contents of computer hard drives and other storage devices owned, operated, or maintained by the district may be accessed by the system administrator(s) without prior notice.

5.4 The system administrator(s) may block messages or remove files that are unacceptable and/or in violation of board policies or operational procedures.

5.5 The system administrator(s) will not intentionally inspect the contents of users' email, or disclose the contents to anyone other than the sender, or intended recipient, without the consent of the sender or intended recipient, unless required to do so by law or the policies of the district, or to investigate complaints regarding electronic files which are alleged to contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material. The district will cooperate fully with any participating district, local, provincial, or federal officials in any investigation concerning or relating to any electronic files transmitted on district information systems.

5.6 In cases where files have been accessed, efforts will be made to inform users within a reasonable time period of any action that is taken.

6. Personal Safety and Information Safeguards

6.1 District staff will ensure that any and all personal information in its care is used and stored in accordance with Operational Procedure 143 (Freedom of Information and Protection of Privacy).

6.2 Users will not repost, copy, forward, or otherwise distribute any information from a district confidential database, including, but not limited to, student, (example: Individual Education Plans), financial, payroll, or personnel, to unauthorized persons.

6.3 District staff will not post student personal information without the consent of the student's parent/guardian or of the student if of legal age. This includes a student's address, telephone number, school address, work address, or any information that clearly identifies an individual student.

6.4 In the case of email, district staff should exercise caution and use the blind carbon copy (BCC) field when sending emails to students or parents/guardians to ensure that they do not violate addressees' privacy by inadvertently sharing email address information.

6.5 Students are not to post personal information about themselves (unless they are of legal age) or other people. Personal information includes their address, telephone, school address, work address, etc.

6.6 Students and parents need to be aware that harassment and bullying occurs on the Internet and that students are to report any incidents to their parents. Parents are to report such activity to the appropriate authorities.

6.7 Students should promptly disclose to their teacher or other district employees any messages users receive at school that are inappropriate or make them feel uncomfortable.

6.8 Where online software or utilities (other than Microsoft 365) are going to be used for educational purposes, they must be FIPPA compliant, and schools must obtain the necessary parental consent (SD72 Form 140-3 is required). If consent is not granted, teachers must provide an alternative learning option.

6.9 Individuals may not use personal devices to record, transmit or post photographic images or video of staff or students during school hours or during school activities without consent as referenced in 6.8.

7. Security

7.1 Network and email use is restricted to only those users that have been issued an authentic username and password by the school district's information technology department.

7.2 Users are responsible for their access to information systems and must take all reasonable precautions to prevent others from being able to use it. It is the user's responsibility to protect all accounts from unauthorized use. For example, users should not write any password on a post-it note and leave it in view or save a password in a password list.

7.3 Under no condition are users to provide their password to another person other than a system administrator.

7.4 Users should not leave a district account open or unattended at any computer system and are to log off their workstations when not in use to avoid unauthorized access.

7.5 Users will immediately notify a system administrator or principal if they have identified a possible security problem. Do not demonstrate the problem to others.

7.6 Attempts to login to the system using another user's identity or as a system administrator may result in disciplinary action.

7.7 Users must not make use of anti-security programs such as, but not limited to, keyboard loggers, password crackers, or unauthorized remote access software.

8. Respecting Resource Limits

8.1 The primary use of district information systems is for educational, career and professional development and the business activities related to operation of the district. Reasonable limits may be imposed to safeguard the efficient operation of the system and to respect the rights of all users.

8.2 Email or other files stored on a district file server are not considered private property and may be removed by a system administrator.

8.3 Users should not download large files unless absolutely necessary. If necessary, download the file at a time when the system is not being heavily used, such as after class or business hours, and immediately remove the file from the system computer to removable media. Users may be asked to terminate a large download if such activity impairs the efficient operation of the system or an educational activity.

8.4 Users will not download, install and/or use any unauthorized peer-to-peer file sharing software.

8.5 Users will not download, install and/or use any unauthorized gaming software.

8.6 Users should check their email frequently, delete unwanted messages promptly, and stay within their account quota as assigned by their system administrator.

8.7 To safeguard the resources of a network system the system administrator may set a disk quota that users will have to adhere to.

9. **Acceptable Use**

9.1 Any staff, students and guests using the district information system, including email, network access and/or Internet access, even if on a personal device, must agree to abide by this operational procedure and complete an Acceptable Use Agreement (Form 140-1) prior to being issued an authentic username and/or password by the school district's information technology department to use the district information system.

9.2 Any use of the school district network for receiving or sending defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, bullying, racially offensive or illegal material, or other inappropriate activities is strictly prohibited. Individuals are strongly encouraged to report any abuse to the appropriate authorities.

9.3 District employees are prohibited from sending jokes, rumours, gossip, or unsubstantiated opinions via email. These communications can be easily misconstrued when communicated electronically.

9.4 If student users mistakenly post information that might be considered inappropriate, they are to immediately tell their teacher or other district employee. If staff mistakenly post information that might be considered inappropriate, they are to immediately tell their supervisor or system administrator. This may protect them against a claim that they have intentionally violated this operational procedure.

9.5 The use of the district's network/email system to solicit for any purpose, campaign for a political candidate, espouse political or social views, promote a religious cause, advertise the sale of merchandise, or for private or non-school district business use is strictly prohibited.

9.6 Employees are prohibited from sending district-wide email messages to all staff. Messages to all staff are to be limited to only necessary correspondence and must be reviewed and authorized by the superintendent or manager of communications prior to distribution.

9.7 Sending email to staff distribution lists at other schools/worksites is generally discouraged. Employees are to be considerate of colleagues' time and consider the legitimate need for a recipient/group to receive a message before sending.

9.8 Network users should not engage in sending messages and files containing any form of digital information or encoding that is likely to result in loss or disruption of the recipient's work or system.

9.9 Network users will not engage in gaining access to any resources, entities or data of others for any purpose without authorization.

9.10 Network users should not engage in activities that are wasteful of network resources or that degrade or disrupt network performance including other networks or systems accessed over the Internet.

9.11 Downloading or the transmission of pornographic, obscene or other socially unacceptable materials is strictly prohibited.

9.12 Any attempt to circumvent system security, guess passwords or in any way gain unauthorized access to local or network resources or to bypass network filters is prohibited.

9.13 Users will not plagiarize works that they find on the Internet and will respect the rights of copyright owners. Refer to Operational Procedure 142 (Copyright) for additional information.

9.14 Staff will install software on a classroom computer or computer system assigned for their use only where they are permitted to do so. Such software must be legally licensed, and a privacy impact assessment should be considered and may be required.

9.15 Users must not install software that they have purchased for home use on a district system, unless they remove the software from their home computer and donate the license, media, and documentation to the district

9.16 Users must not install software that does not have a legal license on a district system.

9.17 Users must not utilize district-licensed software on personal owned systems. The exception is Microsoft 365 while employed. There are terms and conditions with this application – please reference the most up to date guidelines from Microsoft.

10. System Administration

10.1 While circumstances might dictate that a system administrator must investigate or remove files or hardware from a computer or network without prior notice, effort will be made to inform users within a reasonable time period of any action that is taken.

10.2 The district may set quotas for disk usage on any of the district information systems. Users who exceed their quota will be advised to delete files to return to compliance. The users may request that their disk quota be temporarily increased by submitting a request to a system administrator stating the need for the quota increase. After fourteen (14) days' notice, a system administrator may remove any excess files.

10.3 The system administrator(s) may set filters for viruses, SPAM, inappropriate content in email, email attachments and files. Such material may be deleted from the systems by the system administrator(s) without prior notification.

10.4 The system administrator(s) may block ports on the district firewalls and routers that will prevent certain Internet services from being accessed from district computers. These services would be those deemed to be of little or no educational value and/or those that may compromise network performance or security and/or are illegal. Users may request by letter or email that the system administrator(s) unblock a port. The request must include the educational reasons for the required access and the duration of the access.

10.5 The system administrator(s) may delete, remove, or uninstall any software that is unlicensed or illegal or compromises system or network performance or security without prior notification.

10.6 The system administrator(s) may remove any electronic device that compromises system or network performance or security from that network system without prior notification.

10.7 The system administrator may suspend or terminate a user's access to, and use of, any district information system upon breach of the board policies and operational procedures.

10.8 Prior to suspension or termination, or as soon after as is practicable, the system administrator will inform the relevant principal or department manager, who in turn will inform the user of the suspected breach and give the user an opportunity to present an explanation before deciding on a course of action that is in keeping with board policies and operational procedures.

10.9 Any server-based or Wi-Fi information system must be registered with the school district technology department. This will allow for the proper configuration on the network system and monitoring of resource utilization.

11. Personal Responsibility

11.1 Inappropriate or prohibited use may lead to suspension or termination of user privileges, legal prosecution, or disciplinary action appropriate under any applicable laws, policies, regulations, collective agreements, or contracts.

11.2 If an employee receives a message containing defamatory, obscene, menacing, threatening, offensive, harassing, or otherwise objectionable and/or inappropriate statements and/or messages that disclose personal information without authorization they must not forward it and notify their supervisor, the HR department, and the director of information technology about the message. Handle the message as directed by management.

11.3 A user is liable for the costs of any damage that they may maliciously inflict on any district computer system. That damage may include physical damage or electronic damage to system files or data or the files or data of another person using the system.

11.4 The user may be liable for the costs of repairing any physical damage or the cost of any technical services required to repair a loss of system functions or data.

12. **Limitation of Liability**

12.1 The district makes no guarantee that the functions or the services provided by or through the district information systems will be error-free or without defect.

12.2 The district will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions to service.

12.3 The district is not responsible for the accuracy or quality of the information obtained through or stored on the system.

12.4 The district will not be responsible for financial obligations arising through the unauthorized use of the system.

12.5 School purchased technology not consulted on with the director of IT prior to purchase will not be maintained by district IT staff.

12.6 The IT department will support assistive technology and will provide support in the form of infrastructure and accessibility but is not responsible for maintaining or troubleshooting personally owned devices.

12.7 The district is not responsible for stolen, lost or damaged personal devices, including lost or corrupted data on those devices. While school staff may help students identify how to keep personal devices secure, students will have final responsibility for securing their personal devices.

13. **Computer and Device Use**

13.1 All computers and devices purchased by a school, or the school district are deemed school district property.

13.2 A borrower assumes responsibility for the district computer or device and must complete and sign an Acceptable Use Agreement (Form 140-1) and, as appropriate, either a Device Borrower Agreement (Form 140-2) or a Teacher Digital Toolkit Agreement (Form 140-4).

13.3 Each person issued a district computer or device is responsible for its security, regardless of whether it is used in a classroom, office, at the person's place of residence, or in any other location such as an automobile, or a hotel. Users should use common sense to prevent damage and theft and make reasonable effort to ensure that the device is secured at all times. Where any of the above requirements is either inappropriate or impractical (e.g., field trips) users are responsible for taking all reasonable steps to minimize the risk of loss, theft, or damage of the computer or device.

13.4 If a district computer or device is lost through extreme negligence or maliciously damaged, the user may be responsible for reimbursing the district for the repair or replacement of the system. Replacement cost will be based on the purchase price of equipment with similar specifications. Repair costs will be based on actual costs of parts and labour. It is suggested that an additional insurance rider be purchased by the borrower to cover a district-owned computer or device in the home.

13.5 Users must agree to take responsibility and financial liability for the signed-out computer or device and associated peripherals until the user relinquishes custodianship by returning and signing in the computer or device and all peripherals.

13.6 District or school provided computers or devices, including cell phones or teacher digital toolkits, must be returned if the employee resigns or takes an extended absence of three (3) months or longer. Employees can request to purchase the computer or device for the outstanding remaining balance.

13.7 Each teacher has the discretion to allow and regulate the use of personal devices within their classroom and on specific projects.

14. Computer and Device Replacement

14.1 District-owned computers and devices will be collected by IT staff upon the replacement with a new computer or device. Collected computers and devices will be housed at the school board office and assessed by IT staff to be re-deployed where needed.

14.2 School purchased computers and devices will stay at the school of purchase to be collected and catalogued by the school principal.

15. Applications and Online Services

15.1 To ensure the online safety and privacy of SD72 students and staff any application or online service used by the district must be vetted and approved prior to use to ensure that they meet required guidelines for use in the educational environment.

15.2 Before completing SD72 Form 140-5 (Online App Vetting Request) the staff member making the request should review the approved apps list posted in the technology section of the district employee portal to determine if the desired app/service has already been approved or if there is another option that would be equally suitable. This is to ensure consistency of apps/services used throughout the district and to avoid duplication.

15.3 To have an app/service that is on the approved list installed on a device submit a request through the IT helpdesk.

15.4 If the app/service is not already on the approved apps list and there is no suitable approved alternative, complete and submit SD72 Form 140-5 (Online App Vetting Request) considering the following:

15.4.1 The Terms of Use and Privacy Policy from the app/service developer (normally found at the bottom of the developer's website homepage);

15.4.2 The cost related to the use of the app, keeping in mind that apps must be installed on all the school devices and single installation is not permitted;

15.4.3 What supports (i.e., training) are required to use the app/service; and

15.4.4 That the app/service is educationally sound and inclusive and aligns with the district's strategic goals.

15.5 The site administrator must approve the purchase of apps/services.

15.6 The staff member making the request will be notified by an email as to whether the request was approved or denied. If the request was approved, they will also be advised on best practices to ensure student safety and how to arrange for installation.

Reference: Sections 17, 20, 22, 65, 85 *School Act*
Freedom of Information and Protection of Privacy Act
School Regulation 265/89
Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act

Related Forms: SD72 Form 140-1 (Acceptable Use Agreement)
SD72 Form 140-2 (Device Borrower Agreement)
SD72 Form 140-3 (Online Platforms: Acceptable Use Guidelines & FIPPA Consent)
SD72 Form 140-4 (Teacher Digital Toolkit Agreement)
SD72 Form 140-5 (Online App Vetting Request)

Revised: January 2023
May 2022