DIGITAL RESPONSIBILITY FOR EMPLOYEES

Background

The Board of Education for School District No. 43 (Coquitlam) (the Board) views the safe and effective use of technology as essential for teaching, learning, and administrative functions. All technology shall be used in support of the vision, mission, and goals established by the Board and will be used to support our primary purpose of educating students through teaching and the administrative functions of schools and the District. The Board recognizes that technology provides access to a wide variety of instructional and learning resources with the benefit of enhancing and transforming educational opportunities.

In this Administrative Procedure, "technology" refers to District technology or technologies, including the District Network, Digital Services and Digital Content. It also includes the use of personal technology when accessing District technology and services, regardless of whether on or off duty. Use of any technology, personal or District, on or off duty, must be consistent with the relevant standards of conduct expected of an employee of the School District.

Procedures

Employees use technology that is provided by their school, the District, or themselves to access school, District, and Internet sites that enhance and enable their work. The Board does not permit the use of District Technology to create, distribute, or access any material which would not be considered suitable for any sector of our clientele. Inappropriate use of technology has the potential to cause significant damage to District Technology, the reputation of the District, and the trust relationship that the District has with its students, their families and the public.

Regardless of the type of technology used or its ownership, and whether access to District Technology is from within or from outside the District, failure to comply with these procedures may lead to corrective action, termination of network access privileges, and discipline up to and including termination of employment.

1. The District's Network is a shared resource and must be used in moderation. From time to time, employees may be asked to limit their access to enable other high priority processes.
2. Access to District Technology and Digital Content shall be by authorized persons.
3. Employees are not to use District Technology for any commercial or personal business purpose.
4. When working for the District, limited personal use of technology is acceptable as long as it occurs on the employee's own time, does not interfere with their own or others' work and learning, and adheres to the requirements in this Administrative Procedure.
5. Employees should not expect privacy when creating and accessing Digital Content stored on District Technology. In addition, Digital Content traversing District Networks is subject to monitoring, inspection, audits, and access at any time, without

notice, for the purpose of systems maintenance, compliance with the Freedom of Information and Protection of Privacy Act, or if misuse is suspected and to ensure compliance with applicable legal or employment standards and responsibilities.
6. The Board has final say for what purpose District Technology is to be used.

When using technology in relation to their role, employees are expected to…

1. represent and conduct themselves, including when off duty, in accordance with the law and in accordance with the relevant standards of conduct expected of the employee group or profession as they would in any other environment where they represent their school or District department.
2. never impersonate, pose as another person, or falsify their identity in any way.
3. use a professional tone in all communications and not use speech and expression that is inappropriate including but not limited to speech or expression which is profane, disrespectful, slanderous, racist, sexist, libelous, insulting, threatening, hateful, unprofessional , discriminatory, harassing or bullying.
4. use all technology and Digital Content in a legal, ethical, and authorized manner, and in compliance with human rights obligations and workplace policies and procedures.
5. never access or distribute any pornography, offensive or illegal material.
6. comply with the Copyright Act, and patent, trademark, and criminal laws.
7. ensure that all Software and Digital Content installed and accessed is authorized and appropriately licensed.
8. use District Technology resources in moderation and in consideration of the needs of others.
9. ensure that technology is protected from computer viruses, Trojan programs, or other malware infections of all types.
10. maintain and respect the security, privacy, and integrity of Digital Content deemed by the Board to be personal, confidential, or protected and not copy, access, or circulate this material without authorization.
11. protect the identity and privacy of students and staff in accordance with their employment responsibilities or as directed by parents, or guardians and authorized by administrators.
12. Ensure any personal information removed from the workplace is adequately secured by password protection or encryption.
13. not take pictures or record videos of others without their permission (required from parents for persons younger than 19).
14. never attempt to vandalize District Technology, or harm or destroy the Digital Content of other persons, the District, or any agencies or other Networks that are connected to the Internet.

When using District Electronic Mail (email) services, employees are expected to…

1. not forward or print messages received, to other users if specifically stated in the message not to unless necessary as part their employment responsibilities or to protect the health or safety of any person.
2. not send charitable opportunity notices to email distribution lists unless authorized by their Supervisor (sending to individuals that they know personally is acceptable).
3. never send solicitation messages for the intent to provide or sell a product or service.
4. never send messages to users in support of a particular political view or position.
5. never send messages considered to be inappropriate, junk mail, spam, chain e-mail, or a pyramid scheme.

When using Social Networking, Collaboration, Blogging, Media sharing tools, in relation to their role, employees are expected to…

1. use appropriate and respectful User Profile pictures, biographies, and other information to represent themselves.
2. not seek out and "friend" or connect with students without a clear educational purpose, a professional account and User Profile, and without first advising parents.

When using District authorized Network Accounts, employees are expected to…

1. be personally responsible for all activity that occurs within their Network Account.
2. keep their passwords private and out of view of others and never share their passwords with another person.
3. logoff or password lock their Computer or Mobile Device when not actively using it.

Role and Responsibility of Supervisors

Supervisors are responsible for monitoring and supervising the work and conduct of their assigned staff including authorizing, overseeing, and ensuring their staff's responsible use of technology and Digital Content. The following are examples of specific responsibilities of supervisors:

1. Ensure that assigned employees read, understand, and comply with this Administrative Procedure, and accept their responsibilities.
2. Ensure that assigned employees understand how to use relevant technology and Digital Content in a responsible and appropriate manner.
3. Model responsible use of technology and Digital Content.
4. Address online behavior that is harmful, unsafe and/or inappropriate using established employee corrective action procedures.

Role and Responsibility of Information Services Employees

As determined by the District, special administrative access to Digital Technology and Digital Content is granted to employees of the Information Services (IS) Department to carry out their duties in support of District Technology. IS employees are subject to a higher degree of due care and responsibility in protecting their Network Account(s) and all Digital Content. This access must be used only to undertake the technical work assigned in support of the District's operation and never to gain unauthorized access to any Digital Content. IS employees must never share with any other person through any means, confidential information or data accessed or observed during the course of carrying out their assigned duties except as may be reasonably required for training, demonstration or employment purposes. IS employees may not use their access for personal reasons or to further their own personal interests. IS employees who observe or discover inappropriate access or use by others have a duty to report such inappropriate activities to their Manager without delay.

Role and Responsibility of Employees with Administrative Access to Computers or Information Systems

As determined by the District, special administrative access to District Technology and Digital Content is granted to designated employees. These employees are subject to a higher degree of due care and responsibility in protecting their Network Account(s) and all Digital Content. These employees must only use their special access to undertake their work assigned in support of the District's operation or their teaching. They must never use their access to gain unauthorized access to any Digital Content and they must never share with any other person through any means, confidential information or Digital Content accessed or observed during the course of carrying out their assigned duties except as may be reasonably required for training, demonstration or employment purposes. These employees may not use their access for personal reasons or to further their own personal interests. **IS employees who observe or discover inappropriate access or use by others have a duty to report such inappropriate activities to their Manager without delay.**

Definitions and Glossary

Technology / Technologies

Blog: a type of Digital Service for writing and posting articles or other Digital Content for the purpose of sharing and conversing with others; includes the ability to create a User Profile

Computer: a machine, typically in the form of a desktop, laptop, Network, tablet, or slate used by people to create, input, access, view, and share Digital Content

Digital Service: an Network service such as interactive websites, electronic mail, online databases, filing systems, student information systems, business information systems, wikis, blogs, discussion boards, bookmarking and tagging, presentation sites, Digital Content storage, etc.

Digital Content: any data, files, pictures, videos, stored on or accessed with Computers and Mobile Devices

Discussion Forum, or Board: a type of Digital Service designed to support online conversations in the form of (primarily) text-based messages; often includes the ability to create a User Profile

Intranet or Portal: a type of Digital Service provided by the District to give employees a private and secure online space to work with Digital Content that requires a Network Account and password to gain access

Internet: the global public Network outside of the District's control that includes all forms of Digital Services and Digital Content accessible for free or for a fee

Mobile Device: a handheld or pocket-sized Computer or cell / smart phone that is usually connected to a Network and typically includes a display screen, usually with touch input or a small keyboard

Network: a collection of Servers, Computers, and Mobile Devices connected together through various transmissions medium to facilitate the digital communications among people and Digital Services

Network Resource: a Computer, Server, or transmission bandwidth

Network Account: a credential consisting of a unique identity and a secret password that grants access to Network Resources, Digital Services, and Digital Content based on established access rights and permissions

Server: a specialized Computer used to deliver one or more Digital Services and to store Digital Content

Social Network: a type of Digital Service that connects (e.g., "friending", following) people to one another for the purpose of posting and sharing knowledge, information, and to encourage learning; often includes the ability to create a User Profile and to upload Digital Content for sharing purposes

Social Bookmarking: a specific form of a Social Network to facilitate bookmarking (tracking) and sharing with others (publicly) of websites through the use of tags or keywords; includes the ability to create a User Profile and to follow other user's bookmarking activities

Software or Apps: the instructions and programming operating inside Computers, Servers, and Mobile Devices to enable them to perform the functions they are designed for

Video, Audio, Photo, Image (media), and Presentation sharing: specific forms of Social Networks that support the uploading and sharing of Digital Content, specifically video, audio (podcast), photo, image, and presentation files; often includes the ability to create a User Profile

Wiki: a type of Digital Service that supports collaborative creation and editing of webpages and Digital Content by authorized users; often includes the ability to create a User Profile

Other
User: persons authorized to access the District and Internet Networks from District and external sites

User Profile: many Digital Services include the ability for the user to create a profile that may include one or more of their full name, a picture, a biography, links to their websites, their email addresses, and other personal information

Reference: Section 65, 85, School Act
Form 140-1 Student Internet Registration Form

Last reviewed: November 2015