AP XXX Technology – Employee Acceptable Use Guidelines Regulation

Legislative References:
Policy Reference:
Collective Agreement References:
Date:

RE: FORMER POLICY 3035R1 TECHNOLOGY – EMPLOYEE ACCEPTABLE USE GUIDELINES REGULATION

In School District No. 51 (Boundary), we have access to a number of electronic media and services, including telephones, faxes, computers, electronic mail, voice-mail, LAN, Intranet and the World Wide Web.

This regulation is to reiterate some of the practices for the older electronic equipment, and to establish clear policies for the use of new or newer electronic communication.

It is important to note that generally all electronic communications carry a signature, in that it can be traced back to the District and often to the individual. Therefore, anything which you do involving any of the electronic tools must bear this fact in mind. Communications should be in the same tone and with the same professionalism that we would expect in face-to-face discussions with any member or colleague.

1. **All electronic media and services are School District property to be used primarily to carry out the business of the District and not for any other purpose.**

2. **Authorized personnel of the District may, at any time, review files on any District owned PC, email, voice mail or the like. On occasion, the District may be obligated to carry out such a review to determine whether there has been a breach of security, violation of District policy, theft, or misuse. However, the District reserves the right to perform such a review at any time without prior notification to an employee for any reason.**

3. **<u>Computer Software and Other Files</u>**

    - The District reserves the right to examine, access, use, and disclose any and all information or data transmitted, received, or stored on any electronic media, device, or service owned or paid for by the District.

    - No software is to be loaded onto any workstation PCs or other District equipment unless authorized by IT personnel. All software installed on the computer network is to be loaded by authorized IT personnel only, unless IT personnel approves the loading of the software and authorizes and instructs employees to install it themselves.

- District approved and installed software on any workstation PC or any other District equipment shall be removed by authorized IT personnel only.

- Software installed on workstation PCs and laptop computers will be regularly audited by IT personnel.

- If an employee requires that a software license for an approved application be installed on a PC, the employee is to contact the IT Dept. for authorization. A representative of the IT department will then schedule installation of the application upon approval of the request.

- Employees are expressly forbidden to take District software licenses home and install them on their home computers, unless authorization is previously obtained from IT management. Employees shall not download any authorized product version updates, service releases, or patches over the Internet and install them onto their workstation PCs or laptop computers unless explicitly authorized to do so. IT personnel will evaluate these items and install or update these products for employees.

- Any employee who requires a piece of unauthorized software to be installed must have authorized IT personnel approve it for installation on the computer network workstation.

- If an employee notices that unauthorized software is loaded on their workstation PC, possibly installed by the individual who previously worked at their workstation, the employee must report the incident to the IT department so that the software can removed.

4. **Computer Hardware**

- Employees are not to install any personal or unauthorized software onto the District's computer network components or onto their PCs themselves.

- If an employee notices that unauthorized hardware has been installed on his or her PC, possibly by a previous incumbent, the employee is to report the issue to the IT Department and confirm that the hardware was previously authorized. If it wasn't, IT personnel will review the hardware and remove it if necessary.

5. **Internet and Other Electronic Media Usage**

- **Employees are to use the Internet for District/School-related purposes. Personal use should be kept to a minimum, and should not in any way interfere with carrying out one's job duties. Personal use during work hours must be limited to matters of significant urgency. In all other cases, the use should occur outside of working hours;**

- **It is strictly prohibited to use any of the District's electronic services at any time for any purpose that does or might reasonably be believed to:**
  i) violate the law
  ii) involve the transmittal*, receipt, or storage of information or data that is or may reasonably be considered to be harassing, discriminatory, or derogatory to any group or individual. This includes but is not limited to jokes, cartoons and "hate" literature.

  (*transmittal involves the receipt or storage of information or data that is obscene or pornographic, defamatory, or is or may reasonably be perceived to be threatening in nature)

- **Email messages must not contain defamatory, unlawful, threatening, pornographic or otherwise inappropriate of offensive material, violate copyright, or represent personal opinions as those of the District or that have content that could create a legal liability or damage the reputation of the District.**

- **Employees are not to use the District's internet services to enter and participate in chat rooms.**

- **Employees are not to download or install any software from Internet sites onto their network PCs, unless they have been given specific permission and instruction about how to download certain software applications they may need, such as Adobe Acrobat Reader or WinZip.**

- **Employees are not to visit websites known for virus infection, such as file-swapping services or other disreputable websites.**

Employees should be aware that their internet usage patterns, along with the sites they visit, may be logged and may be monitored from time to time by the District's IT staff and management. Employees should not have any expectation of privacy.

6. **Unauthorized Access**

   Attempts to "hack" or "crack" or access information for any unauthorized or non-work related purpose are strictly prohibited.

   No employee shall attempt to gain access to network resources such as files or folders for which they do not have network permission. Any employee caught attempting to access areas or data within the computer network that they have not been given authority to access will face disciplinary actions. Any employee who has damaged the computer network or information stored therein by accessing or attempting to access areas within the network for which the employee has no authorization will be disciplined.

7. **Passwords**

   - **All users shall be required to log on to the network with a unique password of at least 8 digits. Passwords shall all be alphanumeric.**

- **An employee must never sign on to the network and allow a non-employee to access the system.**

- **Employees are responsible for their passwords, and will be held responsible for any operational misuse that occurs under their passwords.**

- **It is each employee's responsibility to ensure that passwords remain confidential to him or herself and not to let other persons use their password. Should an employee believe his or her password has been compromised; the employee should immediately notify the IT department to obtain another password.**

- **It is strictly prohibited to utilize another employee's logon id, except with the express permission of that employee and in the presence of the employee whose logon id is being used.**

8. **E-Mail Usage**

To reduce the risks associated with email practices, the following procedures and practices are to be followed and/or observed:

- e-mail systems are to be used for District/School purposes. Personal use should be kept to a minimum, and should in no way interfere with carrying out of one's job duties

- District e-mail should not be used to register for catalogues, contests or other venue where it can be gathered and sold and be a target for spamming

- the contents of all e-mail messages and attachments are the property of the District, and can be reviewed or monitored for proper usage at any time

- message content should be polite and professional at all times since it is associated with the District

- e-mail systems should never be used to forward undesirable or illegal content

- District e-mail systems should not be used to promote or endorse any personal business, business service or product not associated with the District

- exercise caution in opening attachments in incoming e-mail messages and observe all policy statements or regulations concerning virus prevention and safety when using District e-mail systems

- never alter a message received from another employee and then forward it to other employees. This is a serious breach of trust

- do not forward virus warning messages to people because they are often hoaxes and forwarding perpetuates the problem and reflects negatively on the organization

- **do not forward chain-letter e-mail messages that ask recipients to forward them to five or ten friends. Usually these hoaxes serve no other purpose than to clog email systems and reduce District Internet bandwidth availability**

- **all District e-mail accounts will have the following at the end of the following caution in their signature line**

  This electronic mail transmission and any accompanying attachments contain confidential information intended only for the use of the individual or entity named above. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received these communications in error please immediately delete the e-mail and either notify the sender at the above E-mail address or by telephone at 250-442-your work number.
  Thank you

- **Employees are strictly prohibited from hiding or attempting to hide their identity, falsely representing themselves or attempting to represent themselves as someone else when transmitting, receiving, or storing e-mail or other electronic communications.**

- **E-mail messages are not actually deleted, and cannot be considered private. Message may be saved in at least one other location. Any message or data sent or received or stored on District property is the property of the District and may be reviewed.**

- **Employees, including management and technical staff, will not use the District's e-mail system for the purpose of accessing files or communications of others except as permitted under this policy. Examining, changing, or using another person's files, output, or user name without explicit authorization is strictly prohibited.**

9. **Information of a sensitive or confidential nature uploaded, downloaded, or transmitted by an authorized employee must:**
   - **be clearly labeled "confidential" and message settings indicating a confidential sensitivity**
   - **not be transmitted to unauthorized persons or organizations**
   - **not be left on an unattended computer screen for others walking by to view**

10. **<u>Virus Protection</u>**

    Computer viruses are small applications that cause disruption of computer systems. Their effects can range from minor inconvenience to the complete destruction of data and storage systems. Viruses can spread through infected Internet web pages, through email attachments, and on infected media such as floppy disks, flash memory,

DVD's and CD-ROMs. Most viruses require unwitting users' assistance to spread.

To reduce the risk of virus infection, the District has elected to include the following concepts in their end user regulations:

- do not load software or data from home PCs onto District computer systems
- avoid the use of diskettes, USB memory, DVD's or CD-ROMs that are being used for the first time without approval of the IT Department.
- do not visit websites known for virus infection, such as file-swapping services or any other disreputable websites
- do not open any attachments in e-mail messages that are executable files, unless the e-mail message itself makes sense and appears to be something that the sender would issue. If in doubt, contact the IT department before proceeding
- if the e-mail message appears to be highly generic in its subject line contents, body message contents, or it comes from an unknown sender and contains an attachment, or is in any other way suspicious, report it to network operations staff immediately. Do not open or detach the attachment
- do not forward e-mail messages that include attachments and that encourage recipients to send them to a number of their friends and associates
- **all PCs will run virus-scanning software weekly to scan the contents of the local hard drives on users' network PCs. This software will be set up and configured it to check automatically every night for virus library file updates and to automatically download and install these.**

11. **Network Information Storage**

To reduce risks associated with excess burden on network storage media and to ensure that all necessary data is properly stored, employees should be aware of the following:

- employees are assigned specific storage locations on network hard drives. Their particular folders are individually labelled to match their network login IDs. They should not access or use the storage locations without approval of the IT department
- all data files are to be stored on network hard drives. Each employee requiring data storage has a folder corresponding to their login name

- certain types of information should not be stored on network hard drives. This information includes but is not limited to personal files, games, pictures and graphics that are not District/School-related

- all information stored on network hard drives is considered property of the District and employees should have no expectation of privacy about any of the contents stored on local or network hard drives

- data storage use might be monitored if network capacity is used too quickly

- data that requires permanent storage should be stored on network hard drives, not on employees' workstation PC hard drives. Only data stored on network hard drives is subject to routine backup procedures. Failure of a local hard drive will likely result in the loss of any data the employee had stored on it

- if sharing of data is required, this data should be stored in a shared folder, not one belonging to an individual employee.

12. Safeguarding Data on Network Storage Devices

Risks associated with poor data storage and safeguarding procedures include:

a) loss of data

b) theft of data

c) inadvertent sharing of data with unauthorized individuals

d) unauthorized copying of data

To reduce these risks, the District includes these instructions in their end user regulation:

- Employees are not to store sensitive and confidential information on their workstation PC hard drives. Instead, all such data should be stored on network hard drive space. This will ensure that the data is properly backed up and through logon ID, password, and user authentication and access rights, ensure that only authorized employees have access to the data

- Employees are not to store sensitive or confidential data on writeable media. Media such as this provide a low level of security as they can be easily lost, stolen, or copied

13. Computer System Access

Computer Workstations

To prevent unauthorized use of their PCs, employees should undertake the following precautions:

- If not working in a private workspace always log off computers if away from them for more than a few minutes
- log off from computers at the end of the workday and be sure all applications including BCeSIS session are closed down. Computers are to be left running to facilitate the automatic update of the virus scanning software nightly
- network operations staff should manage the relocation of all computer components as well as the installation of all software except as specifically authorized by network operations staff

As a condition of obtaining a password, employees will be required to sign an Electronic Communications Systems in Schools – Employee Acceptable Use Form, acknowledging that they have read, understood and agreed to abide by this policy and that they understand that they are subject to discipline if the regulations are not followed.

Electronic Communications Systems in Schools
Employee Acceptable Use Form

I certify that I have read the Information Technology Policy for Acceptable Use of Internet, Email, Password, and Information Transmittal & Remote Access (End User Regulation) Statement and agree to act in accordance with it. I understand that any breach of the foregoing provisions may be cause for disciplinary actions or dismissal, including reimbursement of any losses to the District attributable to my actions.

_____ _____

Signature Date

- Original to be kept in employee's file
- Duplicate to be given to employee