POLICY #7.90

DISTRICT TECHNOLOGIES AND INFORMATION SYSTEMS

PREAMBLE

n .- a [(P)-6.1 (OL)2.1 (I)-4.1 (C)]TJ 0 Tc 0 Tw 3.513 0 Td( )Tj0.274 0 Td( )TjEMC /P <</MCID 12 >>BDC /TT1 1 Tf12

ot district technologies.

istrict technologies for commercial or criminal purposes.

REGULATIONS

DEFINITIONS IN THIS POLICY

Information Systems and District Technologies means all hardware and software, applications, procedures, processes and controls of the district, used by or in schools or in the operation of the district.

District Staff means employees of the Board of Education of School District No. 41 (Burnaby).

Network means the school district system local and wide area networks, and includes the Provincial Learning Network (PLNet) and internet.

Internet means the public internet.

PLNet means the wide area network that connects over 1800 schools, post secondary, and other public institutions in British Columbia.

User means any person who uses District Technologies, Information Systems, or network, including any district staff, student, trustee, parent/guardian, guest, or volunteer.

STAFF ACCEPTABLE USE

The District Technologies and Information Systems Acceptable Use Regulation for District Staff is intended to ensure District Technologies and Information Systems are used in a responsible, efficient, ethical, secure and legal manner in accordance with applicable laws and school district policy.

District staff must ensure that appropriate measures are taken to ensure the protection of confidential information and to ensure they do not improperly disseminate confidential or third party personal information.

All users must acknowledge their understanding of this policy and agree to adhere to it as a condition of receiving a user account or accessing District Technologies or Information Systems.

In order to be issued access privileges to District Technologies or Information Systems, all users must fill out form F100a District Technologies and Information Systems Acceptable Use Agreement for Staff.

Access to District Technologies and Information Systems is to be used for educational purposes and for conducting school district business only. Use of District Technologies for any other purpose is prohibited including, without limitation, commercial, criminal, obscene or illegal purposes. However, limited incidental personal use is permitted.

Use in violation of this policy may lead to the suspension or termination of access to District Technologies or Information Systems and discipline, up to and including dismissal.

If the school d

Roles and Responsibilities of Parents/Guardians

1. Read and understand the Acceptable Use Policy, and review this policy with your child.
2. Know that district network-based services and technologies are intended for educational purposes.
3. Understand that it is impossible for the district to restrict access to all controversial materials.
4. Report behaviour that is harmful, unsafe and/or inappropriate.
5. Model digital responsibility.

Roles and Responsibilities of Students: DO

1. Use district and personally-owned devices and digital tools for educational purposes.
2. Follow copyright laws and acknowledge and respect the ownership of others for their creative works.
3. Keep your personal information (last name, home address, phone numbers, picture, passwords) private.
4. Respect the privacy of other students and adults.
5. Report uncomfortable, unsafe, or inappropriate behaviour or messages to your teacher or principal.
6. Treat others fairly and with respect.
7. Understand that digital tools such as e-mail, messaging, social networks, websites, wikis, blogs, texting are not guaranteed to be private.

DO NOT

1. Share your passwords.
2. Take and use someone else's identity (their name, password).
3. Falsify your identity.
4. Take pictures or videos of others and share them without their permission.
5. Hurt or mistreat others by what you create or share.
6. Harass, stalk, bully, threaten, insult, abuse, or attack others.

7. Damage computer systems, networks, digital tools or content.

8. Access secure information owned by others without their permission.

9. Use information or work of others as your own without their permission.

10. Use software programs that are not provided by the district or that are not free or purchased by you for your personally-owned device.

11. Use district or personally-owned devices for commercial, illegal, or malicious purposes.

12. Use district or personally-owned devices to operate file sharing services.

13. Access or distribute pornographic or obscene pictures, videos, audio or text.

14. Meet with someone you met online without your parent(s) or guardian(s) approving and going with you.

.....

Date Adopted: 2014-04
Date(s) Revised:

Cross References: *(policies mentioned in*
Statutory: Freedom of Information & Protection of Privacy Act, School Act, Copyright Act, Criminal Code
Other: Forms: F100a - Staff Acceptable Use Policy, F100b - Student Acceptable Use Policy