303/304.1AP Use of Division and Personal Technology

ESTABLISHED: 2011.08.17
APPROVED: 2020.05.13
AMENDED: 2020.05.04 (2013.02.20)
REVIEWED: 2020.01.24 (2012.06.20)

LEGAL REFERENCE:

- FOIPP Act
- Copyright Act
- Canadian Criminal Code

CROSS REFERENCE:

- 303BP Use of Division-Owned Technology
- 304BP Personal Electronic Devices
- 303/304.1AP Exhibit 2 Staff Responsible Use & Protocol Agreement for Technology Use

---

PROCEDURES:

The Board of the Buffalo Trail Public Schools believes that technology, when used appropriately, is a powerful tool to enhance student learning, enabling students to access, work with, and communicate knowledge and information. The Board believes that, with respect to technology, students should have knowledge, skills and attitudes that will support lifelong learning.

DIGITAL CITIZENSHIP

The responsible use of technology by staff and students is the foundation of BTPS' technology policy. The ISTE Nine Elements of Digital Citizenship are provided below. It is the responsibility of school administration that all users in the school will have the knowledge, skills and abilities to:

- be able to participate in a digital society provided to them when they access Division network services;
- have the knowledge and understand the self-protection required to buy and sell in a digital world,

- have an understanding of digital communication methods and know how to use them appropriately;
- learn to use digital technology collaboratively and demonstrate critical thinking in its use;
- consider others when using digital technologies;
- be ready to protect the rights of others and be able to defend their own digital rights;
- consider the risks (both physical and psychological) when using digital technologies;
- be aware of laws, rules, and division policies that govern the use of digital technologies;
- be custodians of their own information while creating precautions to protect others' data as well.

DEFINITIONS:

Network Resources - refers to the Division's entire Wide Area Network (WAN). It also includes, but is not limited to, VM Hosts, file servers, application servers, communication servers, mail servers, fax servers, web servers, workstations, standalone computers, laptops, software data files and all internal and external computer and communications networks that may be accessed directly or indirectly from our network.

User - all staff members, independent contractors, consultants, temporary workers, students, volunteers and other persons or entities who use the Division's network or equipment.

Electronic Information Resources- means all forms of electronic information, its storage and communication, including electronic storage medium (such as disks, diskettes, CD-ROMs, DVD's, server shares, public folders, web sites and news services, and computer screens), content (such as files and documents, database records, multimedia clips, web pages, email, voice mail, chat room and forum discussions, and news items), and electronic communications medium (such as data lines, modem lines, local, wide area and broadband networks, but does not include telephone conversations;

Inappropriate Material- includes but is not limited to:

- any vulgar or lewd depiction or description of the human body except for artistic or historical depictions of nudity or anatomical, scientific or medical information, used in an educational context;
- any material that has been publicly labeled as being strictly for adults;
- any description of any sexual act which is not part of the approved program of studies used in an educational context;
- graphic description or depiction of violent acts including murder, rape, mutilation, torture or serious injury;
- material encouraging the use of any illicit or illegal drugs, tobacco or alcohol, except for material used in an educational context such as drug abuse statistics;
- on-line gambling services;
- crude or vulgar language or gestures;

- material or information that advocates violence against, denigrates, or exposes a person

or class of persons to hatred or contempt because of race, religious beliefs, color, gender, sexual orientation, physical disability, mental disability, age, ancestry, place of origin, marital status, source of income or family status, including historically inaccurate information that vilifies the person or class of person;

- encouragement of, tools for, or advice on carrying out criminal acts, including lock-picking, bomb-making, and computer hacking information;
- excretory functions, tasteless humor, graphic medical photos outside of the medical context and extreme forms of body modification such as cutting, slashing, branding, and genital piercing; and
- any unlicensed media, software, MP3, MP4, DVD movies or any other copyrighted materials including materials that are bootlegged or illegally available for purchase or download.

Personal Information- means recorded information about an identifiable individual, including:

- the individual's name, home or business address or home or business telephone number;
- the individual's race, national or ethnic origin, color or religious or political beliefs or associations;
- the individual's age, sex, marital status or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, blood type or inheritable characteristics;
- information about the individual's health and health care history, including information about a physical or mental disability;
- information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
- anyone else's opinions about the individual;
- the individual's personal views or opinions, except if they are about someone else; and
- student records or employee records.

Administrative Procedures have been developed for the following Sections:

A. Role of Principal
B. Role of Staff
C Role of Students
D. Access to Network Resources
E. Management of Network resources
F. Intellectual Property and Copyright
G. Outside User Access
H. Consequences

SECTION A: Role of the Principal

1. Ensure all employees at the school receive instruction on BTPS's network procedures.
2. Ensure that staff will not be granted access to BTPS network until they have completed the responsible use agreement.
3. Maintain completed responsible use agreements for students at the school.
4. Ensure that students will not be granted access to the BTPS network until they and their parents have completed the Responsible Use Protocol and Agreement.

5. Establish procedures to ensure supervision of the students using BTPS' network.
6. Where an outside community training program is conducted on the school's network equipment, the principal may authorize such use when satisfied that the Division's network security is ensured.
    a. In the event of an outside agency is using the network no secured logins will be provided or expected.
    b. Software licenses for BTPS are for staff and students and do not include outside agencies.
7. Work with staff to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels and to value and use the information to make their educational goals.
8. Inform themselves and all persons reporting to them about these procedures.

SECTION B: Role of Staff

1. Help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels and to value and use the information to achieve their educational goals.
2. Respect and protect the rights of every other user in the Division and on the Internet.
3. Inform themselves and all students reporting to them about these procedures, including the Responsible Use Protocol and Agreement for Technology Use form.
4. Inform all persons accessing electronic information resources under their control about these procedures.
5. Social networking – professional relationship with students will be maintained at all times. Staff are not to friend students on their personal Facebook, My Space, LinkedIn or iterations of these type of accounts. Furthermore, all electronic communication with a student should be kept in the realm of accepted standards of teacher-student communication.
6. Staff will refrain from texting, checking status on social networking sites, etc., while carrying their assigned duties for BTPS.
7. Must not post, publish, circulate or distribute personal information about themselves or other persons, including family members, teachers, students or friends using any part of the BTPS network unless they have received authorization and the release is in accordance with the Freedom of Information and Protection of Privacy Act.
8. Limited personal use of BTPS electronic information resources is permitted for authorized persons only if it has no negative impact on the performance of the person using the resources and when it complies with BTPS regulations, and the Staff Responsible Use Protocol and Agreement for Technology Use.
9. Persons must not use the BTPS internet servers to post their own personal information anywhere, including to a personal homepage.
10. Persons must not use BTPS electronic information resources to engage in their own business or financial transactions for personal financial gain.

SECTION C: Role of Students

1. Follow and learn the elements of digital citizenship.
2. Will commit to using BTPS network resources in a responsible way by:
    a. Following all guidelines stated on the Student Responsible Use Protocol and Agreement for Technology Use.
    b. Respect and protect the rights of every other user in the Division and on the Internet.
    c. Inform themselves about safety and the use of the internet.
    d. Commit to protecting themselves and their fellow students by not allowing or contributing to cyber-bulling. Furthermore, they will report to a responsible adult any occurrence of these acts.
    e. Never tether or connect together physically or wirelessly their personal devices and any BTPS-owned technology in such a way as to cause the BTPS device to be controlled by the personal device.
3. Must not post, publish, circulate or distribute personal information about themselves or other persons, including family members, teachers, students or friends using any part of the BTPS network unless they have received authorization and the release is in accordance with the Freedom of Information and Protection of Privacy Act.

SECTION D: Access to Network resources

1. Network resources are the property of the BTPS and may be used only for legitimate business or educational purposes. As a general rule, users are permitted access to assist them in their tasks or jobs.
2. Use of the network resources is a privilege, not a right, which may be revoked at any time. Inappropriate, unauthorized or illegal use will result in suspension or cancellation of those privileges. Further disciplinary action may be taken by the Superintendent or designate as deemed appropriate.
3. Use of the network resources shall be consistent with the mission of BTPS and provincial curriculum requirements, taking into account the varied instructional needs, learning styles, abilities and levels of the students.
4. All use of the network resources by any person must comply with any federal, provincial or municipal laws and be in accordance with BTPS and school policies.
5. The information gained or found using the network resources by users does not imply endorsement of the content by BTPS nor does BTPS guarantee the accuracy of the information through the Internet.
6. All users who use BTPS computers shall be responsible for any unauthorized charges, fees, cost damages or injuries resulting from their use of the network resources or in accessing the Internet.
7. All users are responsible for safeguarding their passwords. Individual passwords are not to be printed or given to others, unless the Division grants exceptions in this regard.
8. Users are responsible for all transactions made using their passwords. No user may access the network with another user's credentials. Exception to this is granted to technology staff in attempts to assist users or senior administration for legal purposes.

9. The use of passwords does not imply that users have an expectation of privacy for the material they create.
10. Users using mobile devices that have BTPS data on them must ensure that they are encrypted.
11. Users using personal devices (including personal storage devices) to store BTPS data without encryption are liable for any costs related to loss of personal data.
12. Encryption keys to all BTPS laptops are managed by Technology department.
13. Any personal devices that have both Wi-Fi and data plans through another supplier will not connect directly to our BTPS secure network.
14 Users must not use the Division Internet services for their own personal affairs or to post personal information.
15. Users understand that by being granted access to the BTPS network they have no expectation of privacy.
    a. Users should have no expectation of privacy for anything they create, store, send or receive through BTPS network.
    b. Users expressly waive any right of privacy in anything they create, store, send or receive on BTPS network. Users further understand that the division may use human or automated means to monitor its equipment and network. This includes, but is not limited to, sites visited by users on the Internet, chat rooms, newsgroups, instant messages, social media sites and material uploaded and downloaded through the network.
    c. Email accounts are neither private nor secure. Email sent to non-existent or incorrect names may be delivered to unintended persons. Email is considered a record under the Freedom of Information and Protection of Privacy Act.

SECTION E: Management of Network Resources

1. All infrastructure development and modifications will be coordinated and managed throughout by the Technology Department, which will establish standards.
2. Software installation must be completed in consultation with the Director of Technology, subject to the following conditions:
    a. Appropriate licensing and permissions must be obtained prior to installation.
    b. All software must be licenses in the name Buffalo Trail Public Schools.
    c. Evidence of all software licenses purchased must be readily available for audit. It is the responsibility of the school of department to maintain such evidence.
    d. No personal software may be installed onto the network or the division-owned devices.
3. Network and computer storage devices, servers, backup servers and virtual servers are all the property of BTPS. Network administrators may review any or all files and communications to ensure system integrity and responsible use of resources.

SECTION F: Intellectual Property and Copyright

1. Division electronic information resources are the property of the Division
2. All users of the network resources are required to respect copyright/licensing laws and regulations. The Board will not accept responsibility for a user who willfully and knowingly contravenes copyright or licensing laws.

3. Works covered by copyright that are developed by employees in the course of their employment shall be the intellectual property of the Board.
4. Works created by an employee outside of school facilities beyond the instructional day utilizing Division equipment, licensed software or expertise garnered on the job can be held as to be belonging to the Board.

SECTION G: Outside Users

1. Technology supplied to BTPS classrooms is for the use of students, staff and educational and administrative activities that these users need to carry out the business of schools.
2 Principal may allow limited access to the equipment at their discretion under the following caveats:
    a. If signing on to the network (either wired or wireless) the person will use a guest account.
    b. Said use will not interfere with student and staff access.
    c. Costs created by outside users will be paid by them.
    d. Outside users will abide by the Responsible Use Agreement and policy 303BP Division Owned Technology and 304BP Personal Electronic Devices.
    e. If connecting to a SMART Board the outside user will be responsible for supplying all cables and software needed to operate a Smartboard.
    f. Outside users will not have printing services. g. Outside users will understand that our Internet is filtered and shall not expect exceptions or have the rules altered to allow access to blocked sites.
3. Parent Portal: The Parent Portal is provided as a service to the parents of students enrolled in BTPS schools. Service is controlled by Student Information Services and all enquiries must be directed to this department. Parents/guardians will be informed by their school of what information will be made available to them through parent portal. BTPS requires strong passwords and requires parents/guardians who qualify for access to create a strong password for their Parent Portal access. Once the password is created the parent is the sole owner of the password and is responsible for its security. The School or Divisional office has no record of this password. Any parent using Parent Portal to communicate with staff does so understanding the BTPS Administrative Procedure 401.2AP Bully/Personal/Sexual Harassment. BTPS can at any time remove the privilege of use of the portal due to inappropriate use and/or harassment of staff as stated in our divisional policies.

SECTION H: Consequences

The board desires that violations of these procedures follow a differentiation between age of offender (for students) and employment status (for employees of BTPS and volunteers). Any violation of these procedures, or the principles or expectations set out in it, may result in

a) loss of access privileges;

b) loss of volunteer position;
c) student disciplinary measures under BTPS student discipline policy and 304BP Personal Electronic Devices;
d) employee disciplinary action such as employment suspension or termination; or
e) legal action, including actions taken by the Buffalo Trail Public Schools, by persons unrelated to the Buffalo Trail Public Schools, and criminal prosecution.