Required Descriptor Code: ACDA

Responsible Use

Scope

This policy refers to responsible use of technology and communication tools in Bismarck Public Schools.

Staff and Student ("users") use of technology and communication tools include:

- District owned/provided equipment and services
- Personally owned devices using district accounts, used on district owned/rented/contracted property (including busses) and at district affiliated events
- Any device on any network when the uses is classified as Bullying (ACEA) or Hazing (ACEB)

Examples of tools include, but are not limited to:

- Computers, tablets, and related peripherals
- Internet accessibility from local, wide, virtual, and cellular networks, including wireless
- Local and internet hosted file and application services
- Cell phones, telephones, and multifunctional printers
- Video, audio, and recording technologies

Monitoring Use

The use of electronic resources, technologies, and the internet, whether district owned or personal, on district owned/rented/contracted property is a privilege not a right. All use must be in support of education and consistent with the educational goals, objectives, and priorities of Bismarck Public Schools (BPS). All tools and use shall be subject to the same scrutiny as school lockers for students. Staff shall have no reasonable expectation of privacy when use falls under that defined in "Scope." All use, as defined under "Scope" may be monitored to maintain the integrity of the system and to ensure proper and responsible use. Teachers and administrators will exercise supervision of student use and educate students on responsible use. It is expected students also self-monitor and comply with this policy, rules, procedures, and guidelines.

Requirements for Staff

- *Purpose:*
  Bismarck Public Schools employees are provided or allowed use of technologies as defined under "Scope" for educational purposes only. All employees are expected to communicate and use devices in a professional manner.

- *Use of Electronic Communication Devices:*
  The District monitors internet and all device use defined under "Scope" to prevent or detect abuse and avoid legal exposure.

All employees are authorized to use the internet on the district's network and technology devices for a purpose related to their employment or positions. Limited non-work related use is acceptable provided it:

- Does not interfere with the performance of the employee's duties;
- Does not incur any additional cost to the District beyond standard internet operational costs;
- Does not create the appearance of impropriety;
- Is not for a political or personal commercial purpose;
- Is reasonable in time, duration, and frequency;
- Makes only minimal use of hardware and software resources;
- Is used in accordance with the standards of conduct delineated below.

- *Standards of Conduct*:
  An employee is solely responsible and shall be personally liable, legally, financially, or otherwise, for his or her own misuse of the district's systems/networks, district technology, and/or district internet. Disciplinary action associated with improper use, negligence, or loss of equipment may include being billed for repair or replacement costs, reducing or revoking technology use privileges, or termination.

  - Administration may deem misuse to have occurred when an employee violates any of the following standards of conduct. Violations occur when employees do any of the following using district tools or personal tools on district owned/rented/contractor property as defined under "Scope":
    - Employee use must be professional and ethical;
    - Employee use must not include gambling or betting;
    - Employee use must not be construed as harassing, bullying, insulting, threatening, alarming, or attacking to/of others;
    - Employee use must not be to access, display, archive, store, distribute, edit or record sexually explicit material;
    - Employee use must not be to create, download, or distribute immoral, obscene, threatening, defrauding or violent text or images or transmit inappropriate or unlawful materials;
    - Employee use must not be to create, distribute, copy or knowingly use unauthorized copies of copyrighted material, software, music, images, photos, or video; store such copies on district technology/computers, or transmit them over the district or state networks;
    - Employee use must not be for illegal activity;
    - Employees must not knowingly distribute viruses, bypass any detection system in place, or otherwise damage district-owned technological equipment;

- Employees must not use another's account information, share account information, represent oneself as another, or trespass into another's folders, work, or files;
- Employee must not deliberately or negligently cause damage or loss to any district-owned device;
- Employees must protect themselves, others, and the district by learning and practicing safety with regard to phishing/spam, and data sharing.
- Employees should be aware that technology use as defined under "Scope" is, with limited exceptions (e.g. information pertaining to student's educational record), public information and is likely subject to disclosure per North Dakota's Open Records Law;
- Employees must comply with the district's policy on confidentiality (DEBA) when using technology as defined under "Scope."

Other employee use deemed by administration to be disruptive, inappropriate, or not in the best interest of the District, its employees, and students will be subject to disciplinary consequences.

Requirements for Students

- *Education:*
  The District shall provide education to students about appropriate online behavior, including interacting with other individuals on social networking websites and cyberbullying awareness and response.

- *Prohibitions:*
  Administration or designee may take disciplinary measures when any of the following actions occur while students are using technology tools as defined under "Scope." Disciplinary action associated with improper use, negligence, or loss of equipment may include being billed for repair or replacement costs or reducing or revoking technology use privileges.

  - Using obscene language;
  - Accessing, creating, requesting, or distributing pornographic files or sites and/or other inappropriate material;
  - Harassing, bullying, insulting, threatening, alarming, or attacking others;
  - Damaging computers, computer systems, or computer networks;
  - Violating copyright, trademark, trade secret, or other intellectual property laws;
  - Using or participating in personal and/or non-curricular uses when that use is in violation of stated or written rules or regulations;
  - Using another's account information, sharing your account information, representing oneself as another, or trespassing into another's folder, work, or files;
  - Intentionally abusing network resources;

- Employing the network for political purposes as defined by state law, financial gain, and/or commercial purposes;
- Revealing anyone's personal information such as, but not limited to, an address or phone number without appropriate consent;
- Other activities or actions deemed inappropriate and not in the best interest of the District, its employees, and students.

Off-Campus Technology Usage

BPS reserves the right to extend their authority to off campus staff and student speech that could reasonably come onto the campus and create disruption of the school functioning and/or substantially interfere with the rights of others. Any student conduct on or off campus that could be classified as Bullying (ACEA) or Hazing (ACEB), is subject to the disciplinary actions defined in those administrative policies. This includes, but is not limited to, staff/student created websites, social network postings, blogs, electronic messaging.

Violations

BPS reserves the right to actively monitor staff or student use of technology as defined under "Scope" to ensure compliance with this policy and shall investigate any suspected or alleged violation. Violation of this policy will result in disciplinary consequences as determined by the designated administrator, supervisor, and/or teacher. Disciplinary actions may include, but are not limited to:

- Loss or limits to technology access as defined under "Scope";
- Removal of students from classes with loss of credit;
- Termination of employment;
- Expulsion;
- Billing for costs associated with repair or replacement of equipment associated with improper use;
- Additional disciplinary action may be determined at the site or district level in line with existing discipline procedures;
- When applicable, law enforcement agencies may be involved.

Internet Filtering and Online Safety

Bismarck Public Schools participates in internet filtering services to help restrict access to internet content that is obscene, pornographic, or harmful as defined by the Children's Internet Protection Act (CIPA). Although a filtering system is in place to limit user access to potentially objectionable material, no filtering system can provide complete protection and it is the user's responsibility to access internet resources appropriately. Users accessing the internet through personal cellular connections or other non-district networks and who are on/using district owned/rented/contracted property (including busses) and/or at district affiliated events must adhere to the same filtering restrictions by avoiding internet sites that would be prohibited under CIPA, including those with visual depictions that are obscene, show child pornography, or are harmful to minors. Staff are responsible for supervising students using internet resources.

Concerns/problems with the district filtering system should be reported immediately to the district Technology Department.

Bismarck Public Schools instructs students about appropriate online behavior, including interacting with other individuals on social networking websites, awareness of and response to cyberbullying, and the construction and use of strong/secure passwords. This instruction is conducted yearly through district library media specialists, counselors, teachers, and online materials.

Legal Disclaimer

BPS will not be responsible for damages users may suffer, including loss of data resulting from delay, non-delivery, or service interruptions; damages to personal property used to access school computers, networks, or online resources; or unauthorized financial obligations resulting from use of school accounts to access the internet. BPS specifically denies any responsibility for the accuracy or quality of information obtained through internet services.

Since all transactions conducted through district technology resources could be perceived as authorized district activities, users of district technology resources are responsible for respecting and adhering to local, state, federal and international laws. Any attempt to break those laws through the use of district technology resources may result in legal action against the offender by the district, injured third parties and/or governmental authorities. If such an event should occur, the District will fully comply with proper requests for information related to the legal proceeding, subject only to prohibitions of law. The Bismarck Public Schools will not be held liable for the actions of users, which violate the conditions of this policy.

Complementary Documents

- FFK, Suspension and Expulsion
- FFK-AR, Suspension and Expulsion

End of Bismarck Public School District Policy ACDA

Adopted: 7/1/2015
Revised: 4/7/2020