Bloomfield Public Schools
Technology Acceptable Use Guidelines

Overview

The purpose of this document is to outline the acceptable use of technology assets at the Bloomfield Public Schools. Technology assets including computer equipment, software, storage media, and network account information are the property of the BOE and are to be used to serve the business and educational interests of the district, our employees and students in the course of normal operations. Please refer to the district web site for further information on BOE policies and other technology guidelines including:

- BOE Policy 4725 – Notice regarding electronic monitoring
- BOE Policy 4750 – Policy regarding employee use of the district's computer systems
- BOE Policy 4750.1 – Administrative regulations regarding employee use of the district's computer systems

The Bloomfield Public Schools (BOE) are committed to providing staff with a secure and productive technology environment, free from illegal or damaging actions by individuals, either knowingly or unknowingly. Effective security is a team effort involving the participation and support of every BOE employee, student, and affiliate using our information systems. It is the responsibility of every staff member to understand these guidelines and to conduct their activities accordingly. These rules are in place to protect the students, employee and BOE. Inappropriate use exposes the BOE to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

These guidelines apply to employees, contractors, consultants and visitors to BOE buildings, including all personnel affiliated with third party vendors. They apply to all technology equipment that is owned or leased by the BOE as well as any non-BOE owned equipment that may be connected to our network.

Data Retention – Legal Discovery

Email has become the universal communication tool for staff, students and parents. It is important to note that communications sent via email are subject to the same security and document retention laws as non-electronic correspondence. Therefore all official communication must be sent from a district email account. Similarly, the use of USB and portable storage devices is allowed in district but care should be taken to properly secure data. Keep in mind that sending files to your personal equipment (data-enabled phone, usb drive or home computer) can make these devices discoverable in the event of a legal issue, so it is best practice to not use your personal equipment to transfer or store files.

Monitoring

While the BOE desires to provide a reasonable level of privacy, we reserve the right to monitor and review any material on any machine at anytime in order for the district to ensure appropriate use of network services. The BOE reserves the right to conduct monitoring of these computer systems and can do so despite the assignment to individual employees of passwords for system security. Any password systems implemented by the district are designed solely to provide system security from unauthorized users, not to provide privacy to the individual system user. The Technology department regularly scans shared space and user folders as a group for viruses and other unapproved file types. To ensure that electronic monitoring is not abused, approval from the Assistant Superintendent is required prior to initiating monitoring of a user's electronic communications.

Security and Proprietary Information

1. Information kept on the district network or as a hosted service should be considered private and should not be disclosed without proper authorization. This includes but is not limited to: any student data or lists, employee personnel data, health information or files. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System passwords will be changed quarterly except during the summer months.
3. When you are not at your desk please lock or log off your computer to prevent other users from accessing your data.
4. Because portable computers are especially vulnerable, special care should be exercised. Remember that notebook computers are for educational or business purposes and the same rules apply outside the district as inside.
    a. Portable computers are intended for use in the employee's workspace during normal working hours. After hours they need to be secured by the assigned user.
    b. When used offsite employees are responsible for securing assigned equipment. If damage or theft occurs the employee will:
        i. Report theft to the police in the appropriate jurisdiction and provide a copy of the police report to their administrator
        ii. Complete a BOE incident report within one business day of the damage / theft
        iii. Be financially responsible for lost or stolen equipment in their possession.

5. Even though the district employs multiple levels of anti-virus / anti-spam software, employees must use caution when opening email attachments. It is best practice to contact the sender to verify its source and contents before opening.
6. Local access to the district network is designed for district-owned equipment and approved visitors. Connecting personal equipment to the network is forbidden and may result in the equipment being confiscated without additional notice. Note: Remote access through the district web site has no hardware restrictions.

Unacceptable Use

Under no circumstances is an employee of the BOE authorized to engage in any activity that is illegal under local, state, or federal law while utilizing BOE-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, intellectual property, or similar laws but not limited to:
    a. The installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the BOE.
    b. Unauthorized copying of copyrighted material such as digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music,

2. Introduction of malicious programs into the network, be it on a server, or workstation (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
3. Using a BOE computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
4. Making fraudulent offers of products, items, or services originating from any BOE account.
5. Running a personal business using the BOE's computer resources.
6. Effecting security breaches or disruptions of network communication. Security breaches include but are not limited to:
    a. Connecting an unauthorized wireless access device to the BOE wired network;
    b. Accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
    c. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
    d. Port scanning or security scanning
    e. Executing any form of network monitoring which will intercept data not intended for the employee's host
7. The unauthorized installation of any software onto district owned computer equipment without prior written approval from the technology or curriculum directors.
8. Use of the equipment by non-employees.
9. Circumventing user authentication or security of any host, network or account.
10. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
11. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means
12. Providing information about, or lists of, BOE employees to parties outside BOE unless this activity is a part of the employee's normal job/duty.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" , chain letters or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. The forwarding of jokes, videos, music, and any other email or email attachment that is not Board of Education related business.
5. Sending official BOE business or documents from any email address other that your district assigned email address is prohibited.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.