File: IIBG

ACCEPTABLE USE POLICY

Purpose:
The Beresford School District (BSD) provides network users access to the district's technology resources. As a district, we support the need for technology resources to be available for fulfillment of the BSD mission and goals.

Students, staff, and other authorized individuals will have access to district devices, electronic communication systems, software, and networks, whether wired or wireless. The ability to use technology resources will further the instructional and operational programs within the school district.

The Technology Coordinator and school administrators reserve the right to make decisions about the interpretation of this policy or relevant event and actions involving technology that are not explicitly covered in this policy.

Definitions:
Technology Resources - Beresford School District's technology resources include but are not limited to the following:

- Network
- Internet
- Computer hardware
- Mobile devices
- Peripheral devices
- Software
- Printers
- Servers
- Stored text
- Data files
- Electronic mail
- Digital images
- New technologies as they become available

Technology Department - For the purpose of this policy, the "Technology Department" is defined as the District Educational Technology Director and any other appropriate employees, contractors, or agents as defined by the Educational Technology Director or District Administrators.

Child Pornography - under Federal Law, is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
2. Such a visual depiction is a digital image, computer image, or a computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
3. Such a visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Child Pornography - under State Law, is any book, magazine, pamphlet, slide, photograph, film, video tape, computer depiction or other material depicting a child under the age of 18 years engaging in a prohibited sexual acts or in the simulation of such act.

Harmful to minors - under Federal Law, is any picture, image, graphic image file or other visual depiction that:

1. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex or excretion:
2. Depicts, describes or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or lewd exposition of the genitals; and
3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.

Harmful to minors - under State Law - Is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:

1. Predominantly appeals to the prurient, shameful, or morbid interest of minors;
2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and
3. Taken as a whole lax serious literary, artistic, political, educational or scientific value for minors.

Obscene - any material or performance if:

1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest;
2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; &
3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.

Authority

The Board declares that the use of technology resources are a privilege and not a right for all users. All technology resources, including digital files, are the property of Beresford School District. Users should not expect or assume privacy of anything, including personal files that are created, stored, sent, deleted, received, or displayed on any technology resource that are owned by Beresford School District. The BSD reserves the right to monitor, track, and log network access and use; monitor District used cloud storage programs; deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The District shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state, and federal officials in any investigation.

The District will not be held responsible for any lost, damaged, or unavailable information, files, or any technology resources while using Beresford's technology resources. BSD will not be held responsible for any unauthorized charges or fees resulting access to the Internet or other network resources.

The Board establishes the following materials, in addition to those stated in law and defined by this policy, are inappropriate for access by minors:

1. Threatening
2. Harassing or discriminatory
3. Bullying
4. Terroristic

The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through the established Board policy, or the use of software and/or server blocking. The district will utilize and enforce protective measures to block or filter out matter that is deemed inappropriate by minors and adults. The protective measures will be used on all devices that has access to the Internet.

Delegation of Responsibility

The Beresford School District will inform staff, students, parents/guardians, and other users about this policy through employee and student handbooks, posting on the district website, and by other appropriate methods. A copy of this policy will be provided to users upon written request.

All users will be required to sign an acceptable use policy acknowledging awareness of this policy and the use of the district's monitoring systems to detect inappropriate use.

Student user agreements will be signed by students and parent/guardian. User agreement may be signed electronically.

Administrators, teachers, and staff have a professional obligation to work together to help students develop the intellectual skills necessary to discern among information resources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals. While creating content, users will create content that is appropriate for their age and developmental level.

All users have the responsibility to respect and protect the rights of every other users in the district and on the Internet.

Building administrators shall make the initial determination of whether inappropriate use has occurred.

The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's technology resources are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:

1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for by minors by the Board.
2. Maintaining and securing a usage log.
3. Monitoring online activities of minors.

The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including:

1. Interaction with other individuals on social networking, direct messaging applications, and video conference applications.

2. Cyber bullying awareness and response.

Guidelines

Users will only use their authorized accounts on their authorized devices. Users shall respect the privacy of other users on the system.

Safety

It is the district's goal to protect all users of the network from harassment, unwanted, and unsolicited electronic communications. Any user who receives threatening or inappropriate electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a staff member or administrator. Users shall not revel personal information to other users on the network, direct messaging, email, social networking applications, etc.

Internet safety measures shall effectively address the following:

1. Control of access by minors to inappropriate matter on the Internet or World Wide Web.
2. Safety and security of minors when using electronic mail, direct messaging, and other forms of direct electronic communications.
3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.
4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.
5. Restriction of minor' access to materials harmful to them.

Prohibitions

Users are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically, the uses are prohibited:

- Facilitating illegal activity.
- Commercial or for-profit purposes.
- Nonwork or non-school related work.
- Product advertisement or political lobbying.
- Bullying/Cyberbully.
- Hate mail, discriminatory remarks, and offensive or inflammatory communication.
- Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
- Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.

- Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance tight Board policy.
- Inappropriate language or profanity.
- Transmission of material likely to be offensive or objectionable to recipients.
- Intentional obtaining or modifying of files, passwords and date belonging to other users.
- Impersonation of another user, anonymity and pseudonyms.
- Fraudulent copying, communications, or modification of materials in violation of copyright laws.
- Loading or using of unauthorized games, programs, files, or other electronic media.
- Disruption of the work of other users.
- Destruction, modification, abuse or unauthorized access to network hardware, software and files.
- Accessing the Internet, district computers or other network resources without authorization.
- Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in an authorized access to personal or district files. To protect the integrity of the system, these guideline[1]s shall be followed:

- Users shall not reveal their passwords to another individual.
- Users are not to use a device that has been logged in under another user's credentials.
- Any user identified as a security risk or having a history of problems with other computer systems
- Passwords will follow the guidelines set out by the Educational Technology Director and/or the Administration Team
- All new staff will take the Cyber Training Course in their first year of employment. All returning staff will take the refresher course according to the schedule laid out by the Administration.
- If a user's files/information are held for ransom, the District will not pay the ransom to get files/information returned.

Copyright

The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines and applicable laws and regulations.

District Website

The district shall establish and maintain a website and shall develop and modify its web pages to present information about the district under the direction of the Superintendent or designee. All users publishing content on the district website shall comply with this and other applicable district policies.

Users shall not copy or download information from the district website and disseminate such information on unauthorized web pages without authorization from the Administration Team.

Consequences For Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts

Illegal use of the network; intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services shall be reported to the appropriate legal authorities for possible persecution.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy.

Vandalism shall result in loss of access privileges, disciplinary actions, and/or legal proceedings. Vandalism is defined as any malicious attempt to harm or destroyed data of another user, Internet or other networks; this includes but is not limited to uploading are creating computer viruses.

Failure to comply with this policy or inappropriate use of the Internet, District Network or Computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings.

[May 2014][January 2022]{Reviewed February 2024}