Hankinson Public School Employee Acceptable Use Policy

District Technology

District technology in the Acceptable Use Policy refers to the following categories of technology:
Internet, shared network/file devices; Desktops, laptops, tablets, cameras; Video conferencing, TVs, projectors, phones; Online collaboration, social media, email; Copiers, printers, and peripheral equipment;
and additional technologies as developed.

Section 1: Purpose of Technology Use

The Hankinson Public School District provides technology resources to its students solely for educational purposes. Through technology, the district provides access staff to resources from around the world. The goal in providing these resources is to promote educational excellence in the district by sharing, innovation, and communication.

Section 2: Social Media Use

Social media is to be used within the district as another tool for effective two-way communication. Any site representing the district will be created and maintained by the Superintendent designee. No other entity shall design anything else to officially represent the district in this capacity. No employee shall "friend" a student on any social media sites (except when that student is a relative of the employee).
Social media shall be used:

- To promote the district in a positive manner
- To share District news and information in a timely and relevant information
- To encourage two-way communication between the district and the public
- In ways that are not in violation of policies regarding student safety

Section 3: Privacy

Technology and Internet **access is a privilege**, not a right. Staff shall have no reasonable expectation of privacy when using district computers and/or networks and shall use this technology solely for educational purposes. The district reserves the right to review any content on any device in the building. The district may, for a legitimate reason, perform the following:

- Obtain emails sent or received on District email (K12 or Hankinson Google)
- Monitor an individual's use on District's systems.
- Confiscate or search District owned software or equipment.

This policy applies to school-owned technology on district or personal networks and offline. This policy also applies to privately owned devices that are connected to the district internet and on privately owned networks while on school property. For any legitimate reason, the network administrator may view files and communications (emails, monitor devices) and confiscate any equipment to maintain the integrity of the system and to ensure proper and responsible use of the system. Employees are not allowed to post pictures of students with personal information, and students are not to be "tagged" in photos without permission from the student's parent/guardian. Assume that nothing posted online, in any capacity, is private. Be honest in your online interactions, do not post anonymously. If you are identified as a district employee, be sure to mention your views and opinions are your own and do not represent the district.

Section 4: Monitoring Use

The district believes technology and Internet access play a key role in the education of students; however, the Internet also contains content that is not appropriate for students and staff to access. In accordance with this administrative rule and federal laws such as Children's Online Privacy Protection Act and Children's Internet Protection Act and the Protecting Children in the 21st Century Act, the District has taken reasonable precautions to restrict access to materials obscene, pornographic, and/or harmful to minors using software designed to block sites containing inappropriate material. While the District has taken preventive measures, it recognizes that it is not possible to fully guarantee that students and/or staff will never access objectionable materials. No technology is guaranteed to be safe or totally dependable, nor is it safe when used irresponsibly. The district is not liable or responsible for:

- Any information that may be lost, damaged, or unavailable due to technical, or other difficulties.
- The accuracy or suitability of any information that is retrieved through technology.
- Breaches of confidentiality.
- The consequences that may come from failure to follow District policies governing the use of technology.

Section 5: Password Policy

Passwords are an important aspect of computer security. A poorly chosen password may result in the compromise of Hankinson Public School's entire network. All employees are responsible for selecting and securing their passwords. The purpose of this is to create strong passwords, protect those passwords and the frequency of change.

- All administrative level (administrators, administrative assistants, business manager, technology coordinator, counselor) user passwords must be changed on a **quarterly** basis.
- All user level (staff) passwords (e-mail, computer login) must be changed on a **semester** basis.
- Passwords must be unique and re-use of the same password is not allowed.
- Passwords should never be written down, stored in your classroom, or stored online.
- All passwords must meet the guidelines below:
  - Passwords must **be at least 8 alphanumeric characters** long.
  - Passwords must have **uppercase** and **lowercase** characters.
  - Passwords must have **digits** and **punctuation** characters as well as letters (!@#_03)
  - Passwords should not be based on any personal information such as names of family, pets, friends, our school's name, our school mascot, birthday, address, phone number etc.
  - Make your password easily remembered. One way to do this is by using a phrase or acronym.
  - Do not share passwords with ***anyone.***

Section 6: Mobile Technology

The District Technology is issued to staff for their own personal, school-related uses at school and at home. Any use of the District Technology for other purposes (such as personal purposes) must be minimal.
The district maintains the legal title of any District Technology issues to staff. Staff are authorized to possess and use the District Technology so as they comply with the AUP, but they ***do not have any ownership rights***. Once the District Technology is issued to the staff member, they are responsible for that device ***at all times.*** Any use of personal devices on school property or at school functions is governed by this AUP. Any use may subject contents of the device and any communications on the device to disclosure pursuant or public records request.

With the use of Mobile District Technology:

- Manufacturer defects will be covered by the warranty and/or District.
- Damage or loss that is the result of a staff member's failure to exercise reasonable care will not be covered by the district.
- If damaged, lost or stolen it is not covered by the district or manufacturer, the staff will be solely responsible for paying the replacement and repair costs.
- If the computer is stolen, the police must be notified within twenty-four (24) hours of the discovery of theft. If failure to do so, the user is responsible for replacement.
- Staff members **may** connect their personal phones to the school staff network if they abide by the AUP.
- Personal devices such as own laptops or tablets are not allowed on the school network.
- If the computer is lost or stolen, the user must notify the Technology Coordinator within twenty-four (24) hours of the discovery of loss or theft.
- The district is not responsible if the device is left unsupervised.
- The staff member with that device is **the only authorized user to use it**.
  - They may not share it, trade it, or allow others to use it.
- Staff must bring their devices fully charged and with power cord to school daily.
- Laptops must be used on flat, stable surfaces only.
- Laptops cannot be cleaned with any cleaners with chemicals.
- Laptops must not be marked with markers, stickers, or other materials.
- District applied labels may not be removed.
- Food and drink are not to be used near devices.
- Laptops should not be left in automobiles, as they cannot tolerate extreme heat or cold.

Section 7: Privileges and Responsibilities

This policy outlines the guidelines and behaviors that all users are expected to follow when using technology. It is the responsibility of both Hankinson Public Schools staff members to be responsible members of a digital society that:

- I recognize that use of school technology is a privilege not a right.
- I will practice safe, legal, and responsible use of information and technology.
- I will be courteous, respectful, and responsible to our devices and others around me.
- **I will lock my desk, computer screen and classroom when I am not in my classroom.**
- **As a staff member, I am the only one allowed to log on to my own computer. No student can logon my computer or logon their name to use it.**

(Section 7: continued)

- I will not post any information online that I would not want students, parents, teachers or future colleges/employees to see.
- I will alert the Technology Coordinator if I see anything that is threatening, inappropriate or harmful content.
- I cannot use someone else’s password.
- I cannot go into someone else's account.
- I will abide by such rules as adopted by the Hankinson Public School District #8 Acceptable Use
- Policy Agreement.
- All information and services are available for informational purposes in pursuit of Hankinson Public School District #8 goals.
- I will cooperate, and work with the state and the technology coordinator by informing them of
- inappropriate websites that were accessed accidentally or that need to be blocked to ensure that all CIPA and E-rate rules are abide by.
- I will lock my classroom door, when I am not in the classroom and will use a password protected screen saver on my device.
- I will let students use the computer(s) only when I am in the classroom or computer lab, as the supervisor.
- I release the Hankinson Public School District #8, employees, and administration from any claims and damages arising from my use of the network and the Internet.

Prohibitions

The district subscribes to the acceptable use policies of EduTech. All district computer users shall abide by this policy. The Superintendent or designee may take disciplinary measures when any of the following actions occur:

Using obscene language

- Damaging computers, computer systems, or computer networks
- Accessing or creating pornographic files or sites and/or other inappropriate material
- Any and all purposes that would violate State, Federal or International laws including:
  - Cyberbullying laws (harassing, insulting, or attacking others)
  - Copyright laws (downloading pictures, movies, music, software)
  - Sexting Laws (sending or sharing sexually explicit photos or messages)
- Using or participating in chat lines, chat rooms, and social networking sites for personal and/or non-curricular purposes
- Using someone else's password
- Bypassing or attempting to bypass any of the district’s security or content filtering safeguards.
- Political advocacy
- Trespassing into someone else's folders, work, or files
- Unauthorized use of resources such as servers, networks, computers
- Downloading software unless it is for educational purposes.
- Adding, modifying, repairing, removing, reconfiguring, or tampering with any device on the network infrastructure.
- Interferes with the use of IT resources by the district.
- Interferes with the staff member’s duties or other obligations to the district.
- Intentionally wasting network resources, including, but not limited to, emailing chain letters and/or broadcasting inappropriate messages
- The use of any “hacking tools” that can be used for hacking may not be possessed on any school property or on any District system.
- Employing the network for 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.

Compliance/ Regulations

1. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
2. Family Education Rights and Privacy Act 1974 (FERPA)
3. Copyright Act of 1976
4. Foreign Corrupt Practices Act of 1977
5. Computer Fraud and Abuse Act of 1986
6. Computer Security Act of 1987
7. Children’s Internet Protection Act of 2000 (CIP)

EduTech Acceptable Use

EduTech provides information technology resources to K-12 schools in North Dakota. These resources deliver electronic communications internally within school districts and externally to systems across the world. We provide these services solely to promote and enhance the quality of education in North Dakota's K-12 system.

This acceptable use policy ensures that use of the EduTech resources by all users is done in an appropriate manner. Use of EduTech services is a privilege and not a right. All users are obligated to respect and protect the rights of every other user and act in a responsible, ethical, and legal manner.

Acceptable Use

1. EduTech accounts and affiliated services may be used for K-12 education related purposes only.
2. Logins and passwords are provided for the individual's use while they are affiliated with an EduTech member school or organization,
3. Under no conditions shall any user provide another person with access to or use of their account. Similarly, users shall not examine, change, or use any account but their own. No user may represent themselves as another individual or entity in electronic communication.
4. Users shall not deliberately attempt to degrade system performance or capability. Knowledge of system or special passwords does not convey permission or privilege to use such passwords. No account shall be used to damage a system or file or remove information without authorization.
5. EduTech's services may be used only for lawful purposes. Transmission, distribution, or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.
6. Under no circumstances may EduTech's services be used to send material that is intended to threaten, harass, annoy, or alarm another person without legitimate purpose-this includes chain mail.
7. Use of computer system and databases shall be limited to the purpose(s) for which access was granted. Use of services for political (lobbying) purposes, for gaining business contacts or for personal or private profit is prohibited. Organizations may not use any EduTech service for increasing their membership or gaining additional contacts.
8. Users should expect only limited privacy in the contents of their personal files and communications. Files may be searched if there is reasonable cause that a user has violated EduTech policies or the law. Investigations will be reasonable and related to the suspected violation. EduTech will cooperate with external networks and authorities in the resolution of an investigation within the restrictions of federal and state law and the Family Educational Right to Privacy Act (FERPA).
9. Any user of EduTech's services who violates this policy may be denied access to the system. Users may also be denied access based on their local school district's acceptable use policy.

Failure to abide by this policy may result in the loss of privileges as well as further disciplinary and/or legal action. All accounts are the sole property of EduTech and are provided to the user's organization or school district as a service, as such final determination of account status is up to EduTech staff and may not be appealed. If account access is denied for disciplinary reasons, users forfeit all information in the account.

Hankinson Public School
Acceptable Use Policy
Agreement Acknowledgement

____

Employee Name (please print)

Violations of this acceptable use policy or any applicable federal or state law, rule, or regulation may also result in disciplinary action up to and including termination of employment for staff.

Consent

All staff must consent to this policy in writing prior to accessing district networks and/or computers.

I understand that I am representing the Hankinson Public School District #8 and such as, must respect the rights of others, protect the integrity of the information technology, and observe all relevant laws, regulations, and contracts, including software licensing agreements and copyright laws. When using the school district's hardware/software equipment.

I have read and agree to comply with the Hankinson Public School District #8 Acceptable Use Policy Agreement. I understand that any violation of these regulations is unethical, potentially illegal, and may result in criminal offense. Should I commit any violation, my access privileges may be revoked.

____ __________________

Employee Signature Date