RESPONSIBLE USE REGULATIONS OF TECHNOLOGY RESOURCES FOR STAFF & STUDENTS

*Users refer to both WFPS staff and students.

West Fargo Public Schools provides technology resources for staff and students (users) to support the educational mission of the district. Use of these technologies must be consistent with academic actions of the West Fargo Public Schools (WFPS). Users are expected to adhere to WFPS district policy ACDA-AP. Users are required to comply with all local, state, and federal laws including regulations against computer/network hacking, software piracy, copyright infringement and other illegal behaviors.

The district expects users to exhibit responsible behaviors when using WFPS technology resources. The successful use of these resources requires adherence to the policy that promotes efficiency, safety, and appropriate usage. Use of technology resources is a privilege that may be revoked if expectations are not followed. Failure to comply may result in disciplinary actions including termination of employment or suspension.

The WFPS District is responsible for informing and educating users of responsible, safe use of technology. Please review these policies and agree to them to secure access to WFPS technology resources.

Sanctions
Suspected violations of this policy by users shall be reported to Director of Technology, building principal, and/or supervisor. Violations of the West Fargo Public School District Responsible Use Policy are to be treated like any other legal or ethical violation as outlined in applicable staff and student handbooks, and relevant contractual agreements. Violators may also be subject to prosecution under applicable Federal and North Dakota statutes. Any violation of the policy may result in a cancellation of network computing privileges and/or disciplinary action determined by the appropriate authority.

Scope, Authorization, Purpose of Use and General Responsible Use Guidelines
These expectations apply to all users of WFPS technology resources. This includes resources used within the district or those used remotely on district owned/rented/contracted property (including busses) and at district affiliated events.

Technology resources provided by the district include but are not limited to:

- Computers and related peripherals
- Personal technology devices including, but not limited to: tablets, e-readers, iPads and iPods
- Printers of all types
- File and application servers
- Telephones, faxes, and voice mail systems
- Local and wide area networks, including wireless networks
- Internet access
- Email accounts
- Video networks
- Televisions, VCR and DVD players
- Cameras
- Copy machines

Users should take all reasonable precautions to protect the WFPS technology resources. Users may be held financially responsible for damages to district technology resources.

General Rules of Technology Resources

Privacy is not guaranteed when using WFPS technology, including the network. Files, communications (including email), and use history may be reviewed to maintain system integrity and ensure that users are adhering to the responsible use policy and guidelines. The district will cooperate with local, state, and federal authorities when necessary. All technology-related activity could fall under North Dakota open record laws and this may mean that the media could ask to review e-mail communications at any time.

Use of WFPS technology resources must be consistent and in support of the mission of the district in an ethical and professional manner. The school district reserves the right to prioritize use and access to technology resources. Any use of technology resources must conform to state and federal law, provider policies, licensure, copyright and fair use guidelines, and district policy.

WFPS prohibits the use of technology resources for:

- Sending or displaying offensive messages or pictures.
- Using obscene language, sending hate mail, accessing, storing or distributing obscene or pornographic materials.
- Harassing, insulting, bullying, stalking or attacking others.
- Using the system to support or oppose political candidates, ballots or personal agendas.
- Damaging computers, computer systems or computer networks.
- Violating copyright laws including plagiarizing, downloading or exchanging pirated software, music, videos, or other files.
- Using others' credentials (including user names and passwords for both network and applications) tampering with or forging names on electronic mail or other online environments.
- Trespassing in others' folders, work or files. (Exception: A supervising teacher has rights to his/her student teacher's H: drive.)
- Hacking with intent to damage or for the purposes of circumventing standard configurations.
- Intentionally wasting network resources.
- Unauthorized posting of personal information about others, including phone numbers, names, etc.
- Performing any action which results in a compromise of the system security.
- Using the network for any illegal, unethical, personal gain, commercial, or religious activities.
- Negligence regarding confidential data.

***** Unauthorized or irresponsible use of *personal technology device*s by students may result in suspension or revocation of personal device privileges. These uses include, but are not limited to, the following:

- Using personal devices to gain or give an advantage in a testing situation.
- Using personal devices during class that are not approved by the building administrator or the individual teacher and as defined by building expectations.
- Downloading and installing district licensed software on personal devices unless specifically allowed by the licensing agreement.
- Using personal devices to bypass filters, circumvent network security, or violate the responsible use standards which normally apply to district-owned technology.

- Using personal devices for violations related to cyber bullying and harassment.

*A personal technology device includes, but is not limited to: cell phones, smart phones, tablets, e-readers, and laptops.

Data Protection Procedures

Federal law requires organizations that use electronic information to collect, handle, and store information responsibly. Users must:

- Obtain and process data fairly and lawfully.
- Hold data only for lawful purposes.
- Use data only for school related purposes.
- Ensure that any data held is adequate, relevant and not excessive in relation to the purposes for which it is held.
- Ensure that the data is accurate and up-to-date.
- Protect and secure data access, including information sent or received from personal devices (i.e. email accessed from smartphones).

Electronic Mail and Internet Use

- Users must adhere to these guidelines at all times when using the internet and/or email, including after hours, weekend and/or holiday use. Users are prohibited from using district email and/or internet access for commercial / personal gain or religious activities.
- Users are prohibited from using district provided email or internet access for unethical or illegal behaviors or activities that are contrary to any district policy.
- Users are prohibited from forwarding non-school related emails: jokes, chain emails, and non-educational content.

Internet Safety and Use of Filters

WFPS participates in internet filtering services to help prevent access to internet content that is obscene, pornographic, or harmful. Although the district provides a filtering system 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. Students must be appropriately supervised when using district technology resources.

School personnel will follow the district's policies on student staff relations, employee speech, and social media. Educators will promote and model responsible use, digital citizenship and online responsibility to support learning.

Security

Network and computer security systems help maintain the integrity of the district technology resources. Any attempts to circumvent, disable, or misuse security systems are prohibited. It is the user's responsibility to protect their credentials from unauthorized use. This includes, but is not limited to, leaving a computer unattended while you are logged in.

The specific usage guidelines outlined here are not intended to be comprehensive, but rather to establish and clarify the intent of ACDA-AP. Situations not detailed here will inevitably arise, and they should be interpreted according to the spirit of this policy.

NON-STAFF/SPECIAL ASSIGNMENT CONTRACT
WEST FARGO SCHOOL DISTRICT RESPONSIBLE USE OF TECHNOLOGY RESOURCES

Please check one:

___ Student Teacher ___ Long Term Substitute ___ Other (Please describe) _____

Last Name: _____First Name _____MI ____

School / District Location: _____

Position: _____Grade Level: ___Department: _____

Approximate dates account access needed (ongoing, semester dates, etc.) _____

Student teachers, long-term substitutes and others needing staff account privileges complete this section:

Supervising Teacher: _____Grade Level: _____ Department: _____

Supervising Teacher Signature: _____Date: _____

Principal Signature: _____Date: _____

Scan and email Contract with all signatures to shoffman@west-fargo.k12.nd.us or fax at 701.356.2009

I have read the West Fargo School District Computer Network Policy and Responsible Use of Technology Resources Regulation, and agree to abide by the provisions. I understand that violation of the provisions stated in the policy may constitute suspension or revocation of network access and related privileges and could lead to school disciplinary action, including termination of employment.

_____ _____
Staff Member's Signature Date