



FREWSBURG CENTRAL SCHOOL  
26 INSTITUTE STREET  
FREWSBURG, NEW YORK  
Phone: (716) 569-7000

### APPLICATION FOR SUBSTITUTE TEACHER

Name: \_\_\_\_\_  
(Last) (First) (Maiden)

Address: \_\_\_\_\_  
(Street) (City) (State, Zip)

Primary Phone: \_\_\_\_\_ Social Security # \_\_\_\_\_

#### EDUCATION

Name/Location	Dates	Major	Minor	Degree
High School	to	xxxx	xxxx	xxxx
College	to			
College	to			

Number of Hours in Education: \_\_\_\_\_

#### TEACHING EXPERIENCE

District/Location	Dates	Subject/Level	Reason for Leaving
	to		
	to		
	to		

Do you hold a current New York State Certificate? Yes No Number: \_\_\_\_\_

Subject(s) or grades you prefer to teach: \_\_\_\_\_

Check the days you are available for substitute work: M T W Th F

Are you available on short notice? Yes No Comments: \_\_\_\_\_

Have you ever been employed by a school district and released from employment?

Yes

No

If yes, state reason:

REFERENCES (List three – 2 of whom are former employers)		
Name	Address	Telephone

**NOTE:** An UNCERTIFIED SUBSTITUTE may teach only up to 40 days per year. A CERTIFIED SUBSTITUTE must supply this office with a copy of his/her TEACHER'S CERTIFICATE.

PERSONAL BACKGROUND HISTORY		
	Yes	No
Have you ever been convicted of a crime?		
If yes, have you been issued a certificate of relief from disability?		
Are any criminal charges or proceedings pending against you? (If yes to either or both above, please explain on a separate sheet.)		
Have you ever served in the US Armed Forces?		
If yes, did you receive a dishonorable discharge? (If yes, please explain on a separate sheet. A dishonorable discharge is not an absolute bar to employment; other factors will affect the final employment decision.)		

List any persons currently serving on our Board of Education or working for the district who are related to you:

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Date)

## **SUBJECT: EMPLOYEE USE OF COMPUTERIZED INFORMATION RESOURCES**

The Board of Education will provide certain District employees with access to various computerized information resources through any aspect of the District's computer system (hereafter "DCS") consisting of software, hardware, computer networks, wireless networks/access and electronic communication systems. This may include access to electronic mail, so-called "on-line services" and the "Internet." It may also include the opportunity for some employees to have independent access to the DCS from their home, other remote locations, and/or to access the DCS from their personal devices. All use of the DCS and the wireless network, including independent use off school premises and use on personal devices, shall be subject to and governed by this policy and accompanying regulations and related District policies and regulations.

The Board encourages District employees to make use of the DCS to explore educational topics, conduct research and contact others in the educational world. The Board anticipates that employees' access to various computerized information resources will both expedite and enhance the performance of tasks associated with their positions and assignments. To that end, the Board directs the Superintendent or his/her designee(s) to provide employees with training in the proper and effective use of the DCS.

Employee use of the DCS is conditioned upon written agreement by the employee that use of the DCS will conform to the requirements of this policy and any regulations adopted to ensure acceptable use of the DCS. All such agreements shall be kept on file in the District Office and may be viewed by any employee member upon his or her request.

Generally, the same standards of acceptable employee conduct which apply to any aspect of job performance shall apply to use of the DCS. Employees are expected to communicate with common sense and in a professional manner consistent with applicable District policies and regulations governing the behavior of school employees. Electronic mail and telecommunications are not to be utilized to share confidential information about students or other employees.

Access to confidential data is a privilege afforded to District employees in the performance of their duties. Safeguarding this data is a District responsibility that the Board of Education takes very seriously. Consequently, District employment does not automatically guarantee the initial or ongoing ability to use mobile/personal devices to access the DCS and the information it may contain.

This policy does not attempt to articulate all required and/or acceptable uses of the DCS; nor is it the intention of this policy to define all inappropriate usage. Administrative regulations will further define general guidelines of appropriate employee conduct and use as well as proscribed behavior.

District employees shall also adhere to all laws, policies and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements and rights of privacy protected by federal and state law.

Employees who engage in unacceptable use may lose access to the DCS and may be subject to further discipline under the law and in accordance with applicable collective bargaining agreements. Legal action may also be initiated against an employee who willfully, maliciously, or unlawfully damages, steals, or destroys property of the District.

(Continued)

**SUBJECT: EMPLOYEE USE OF COMPUTERIZED INFORMATION RESOURCES (Cont'd)**

The School District recognizes the value of teacher and employee inquiry, investigation and communication using new technology tools to enhance student learning experiences. The School District also realizes its obligations to teach and ensure responsible and safe use of these new technologies. Social media, including social networking sites, have great potential to connect people around the globe and enhance communication. At this time, the only District approved, password protected, social media network site, for classroom use, is "My Big Campus". As technology advances, the District reserves the right to review and ammend this policy.

For purposes of this Policy, the definition of public social media networks or Social Networking Sites (SNS) are defined to include: websites, Web logs (blogs), wikis, social networks, online forums, virtual worlds, video sites and any other social media generally available to the School District community which do not fall within the District's electronic technology network (e.g., Facebook, MySpace, Twitter, LinkedIn, Flickr, Vine, Instagram, SnapChat, blog sites, etc.). The definition of District approved password-protected social media tools are those that fall within the District's electronic technology network or which the District has approved for educational use. Within these internal forums, the District has greater authority and ability to protect minors from inappropriate content and can limit public access.

The use of social media (whether public or internal) can generally be defined as Official District Use, Professional/Instructional Use and Personal Use. The definitions, uses and responsibilities will be further defined and differentiated in the Administrative Regulation. The School District takes no position on an employee's decision to participate in the use of social media or SNS for personal use on personal time. However, personal use of these media during District time or on District-owned equipment is prohibited. In addition, employees are encouraged to maintain the highest levels of professionalism when communicating, whether using District devices or their own personal devices, in their professional capacity as educators. They have responsibility to address inappropriate behavior or activity on these networks, including requirements for mandated reporting and compliance with all applicable District Policies and Regulations.

**Confidentiality, Private Information and Privacy Rights**

Confidential and/or private data, including but not limited to, protected student records, employee personal identifying information, and District assessment data, shall only be loaded, stored or transferred to District-owned devices which have encryption and/or password protection. This restriction, designed to ensure data security, encompasses all computers and devices within the DCS, any mobile devices, including flash or key drives, and any devices that access the DCS from remote locations. Employees will not use email to transmit confidential files in order to work at home or another location. Employees will not use cloud-based storage services (such as Dropbox, GoogleDrive, SkyDrive, etc.) for confidential files.

Employees will not leave any devices unattended with confidential information visible. All devices are required to be locked down while the employee steps away from the device, and settings enabled to freeze and lock after a set period of inactivity.

(Continued)

**SUBJECT: EMPLOYEE USE OF COMPUTERIZED INFORMATION RESOURCES (Cont'd)**

Employee data files and electronic storage areas shall remain District property, subject to District control and inspection. The Director of Technology & Communications may access all such files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy and accompanying regulations. Employees should NOT expect that information stored on the DCS will be private.

**Implementation**

Administrative regulations will be developed to implement the terms of this policy, addressing general parameters of acceptable employee conduct as well as prohibited activities so as to provide appropriate guidelines for employee use of the DCS.

Adopted September 11, 2014

**SUBJECT: EMPLOYEE USE OF DISTRICT COMPUTER SYSTEM**

The District's computer system (hereafter "DCS") is provided for employees to enhance the educational programs of the District, to further District goals and objectives, and to conduct research and communicate with others regarding topics related to the education of students.

Generally, the same standards of common sense and acceptable staff conduct which apply to any aspect of job performance shall apply to use of the DCS. The standards of acceptable use as well as prohibited conduct by employees accessing the DCS, as outlined in District policies and regulations, are not intended to be all-inclusive. Any employee member who commits an act of misconduct which is not specifically addressed in District policy and/or regulation may also be subject to disciplinary action, including loss of access to the DCS as well as the imposition of discipline under the law and/or any applicable collective bargaining agreements. Legal action may also be initiated against an employee who willfully, maliciously or unlawfully damages, steals, or destroys District property or uses the DCS in the commission of a crime.

Employees are encouraged to utilize electronic communications in their roles with the District. Employees are also encouraged to utilize electronic means to exchange communications with parents/guardians or homebound students, subject to appropriate consideration for student privacy. All such usage shall be limited to school related issues or activities. Communications over the DCS are often public in nature; therefore, general rules and standards for professional behavior and communications will apply.

The District's policies and accompanying regulations regarding employee, and student use of computerized information resources establish guidelines to follow in instruction and in working with students on acceptable use of the DCS, including access to external computer networks.

All employees who use mobile technology in the course of their job duties, including but not limited to cell phones, smart phones, flash drives, tablets, e-readers, laptop computers, scanners, printers, digital cameras, camcorders, PDAs, iPads and iPods, shall abide by this Regulation which governs the use of this type of equipment. Any device that runs software or systems including, but not limited to, Palm OS, Windows, Pocket PC, Android, or IOS is considered a "computer" for the purposes of this Regulation. In addition, all applicable language in Policy and Regulation #6471 and #6471R – Employee Use of Computerized Information Resources and Form #6471F – Agreement for Employee Use of Computerized Information Resources (AUP) also applies to mobile and personal technology equipment when it is used in conjunction with the District's wireless network or in the course of the employees job duties.

Access to confidential data is a privilege afforded to District employees in the performance of their duties. Safeguarding this data is a District responsibility that the Board of Education takes very seriously. Consequently, District employment does not automatically guarantee the initial or ongoing ability to use mobile/personal devices to access the DCS and the information contained therein.

(Continued)

**SUBJECT: EMPLOYEE USE OF DISTRICT COMPUTER SYSTEM  
(Cont'd.)**

**Prohibitions**

It is not the intention of this regulation to define all inappropriate usage. However, in addition to the general requirements of common sense and acceptable employee behavior, activities which shall be prohibited by employees using the DCS include, but are not limited to, the following:

1. Using the DCS in any way which results in unauthorized charges or expense to the District.
2. Damaging, disabling or otherwise interfering with the operation of computers, computer systems, software, or related equipment through physical action or by electronic means.
3. Using unauthorized software on the DCS.
4. Changing, copying, renaming, deleting, reading or otherwise accessing files or software not created by the employee without express permission from the Director of Technology & Communications.
5. Violating copyright law or other laws, rules, or regulations.
6. Employing the DCS for commercial purposes, personal gain, marketing, sales, product advertisement, advancement of any personal religious or political belief or creed, any illegal activity, or political lobbying.
7. Disclosing an individual password to others or using any password(s) assigned to or associated with any other user or individual.
8. Sharing confidential information about District students, employees, staff or officials.
9. Sending or displaying offensive messages or pictures, including but not limited to obscene or pornographic messages and pictures.
10. Using obscene language.
11. Harassing, insulting or attacking others.
12. Engaging in practices that threaten the DCS (e.g., loading files that may introduce a virus).

(Continued)

**SUBJECT: EMPLOYEE USE OF DISTRICT COMPUTER SYSTEM  
(Cont'd.)**

13. Violating regulations prescribed by the network provider.
14. Excessive use of the DCS for other than school related work or activities.
15. Assisting a student to violate District policy and/or regulation, or failing to report knowledge of any student violations of the District's policy and regulation on student use of computerized information resources.
16. Use which violates any other aspect of Base School District policy and/or regulations, as well as local, state or federal laws or regulations.

Any user of the DCS that accesses another network or other computer resources shall be subject to that network's acceptable use policy.

**Confidentiality, Private Information and Privacy Rights**

Confidential and/or private data, including but not limited to, protected student records, employee personal identifying information, and District assessment data, shall only be loaded, stored or transferred to District-owned devices which have encryption and/or password protection. This restriction, designed to ensure data security, encompasses all computers and devices within the DCS, any mobile devices, including flash or key drives, and any devices that access the DCS from remote locations. Employees will not use email to transmit confidential files in order to work at home or another location. Employees will not use cloud-based storage services (such as Dropbox, GoogleDrive, SkyDrive, etc.) for confidential files.

Employees will not leave any devices unattended with confidential information visible. All devices are required to be locked down while the staff member steps away from the device, and settings enabled to freeze and lock after a set period of inactivity.

Employee data files, e-mail, and electronic storage areas shall remain District property, subject to District control and inspection. The Director of Technology & Communications or the Superintendent's designee(s) may access all such files and communications, and storage areas, without prior notice, to ensure system integrity and that users are complying with requirements of this policy and accompanying regulations. Employees should NOT expect that information stored on the DCS will be private.

(Continued)

**SUBJECT: EMPLOYEE USE OF DISTRICT COMPUTER SYSTEM**  
**(Cont'd.)**

**Personally Owned Devices**

If a staff member chooses to use his/her own personal technology equipment, the following guidelines will apply:

1. Prior to use on the DCS or wireless network, all devices must be approved by the Superintendent.

OR

Personal devices will only be connected to the guest wireless network and not be connected to the DCS.

\*The District reserves the right to review and amend this policy.

2. The entire cost to acquire all personal technology equipment is the responsibility of the employee. Services that may incur a financial cost to the District, such as phone options, software or other "apps" are not allowed. The District does not agree to pay such charges and employees who desire these options must assume all costs incurred for such charges.
3. Personal technology equipment is not covered by the District's Insurance if it is lost, stolen or damaged. Loss or damage to any personal technology equipment is solely the responsibility of the employee. If lost or stolen, the loss should be reported immediately to Technology staff so appropriate action can be taken to minimize any possible risk to the DCS and the District.
4. Employees assume complete responsibility for the maintenance of personal devices, including maintenance to conform to District standards. Employees also assumes all responsibility for problem resolution, as well as the use and maintenance of functional, up-to-date anti-virus and anti-malware software and any other protections deemed necessary by Technology staff.
5. Employees must also meet any expectations of continuity in formatting of files, etc. when making changes to documents for work purposes (i.e., do not change the format of a file so that the original file is unusable on District-owned hardware/software).

(Continued)

**SUBJECT: EMPLOYEE USE OF DISTRICT COMPUTER SYSTEM**

**(Cont'd.)**

6. All personal technology equipment used on the DCS or wireless network is subject to review by the Director of Technology & Communication, or individuals/entities designated by the Superintendent, if there is reason to suspect that the personal device is causing a problem on the DCS network, or if the employee is suspected by a supervisor of spending excessive time at work on non-work related matters.
7. The District's email client will not be installed on personally owned devices. All access to email will be through the an internet browser. The District reserves the right to review and amend this policy.
8. The use of personal technology equipment in the course of an employees' professional responsibilities may result in the equipment and/or certain data maintained on it being subject to review, production and/or disclosure (i.e., in response to a FOIL request, discovery demand or subpoena). The employee is required to submit any such information or equipment, when requested.
9. It is also the responsibility of the District employee using a mobile device, personal or District-owned, to ensure that all security protocols normally issued in the management of District data on conventional storage infrastructure are also applied on that mobile device. All District-defined processes for storing, accessing and back up data must be used on any device used to access the DCS.
10. Use of any mobile technology device during the school day, whether District-issued or personally owned, should not interfere with the employees' ability to carry out daily responsibilities.

**District- Issued Devices**

Mobile wireless devices issued by the District will be subject to audit and inventory standards. Employees must be able to produce the device when requested by a District official. If the device is lost or damaged, it must be reported to the employees supervisor immediately. If theft is suspected, law enforcement will be contacted.

**Flash Drives**

Flash or key drives may be provided to staff members for use on the District network if requested by their supervisor. These flash drives will not be used for confidential information. Use of personally owned flash drives or other external storage devices to conduct District business is prohibited unless otherwise specified by the Superintendent or a person of his/her designee.

(Continued)

**SUBJECT: EMPLOYEE USE OF DISTRICT COMPUTER SYSTEM**  
**(Cont'd.)**

**Wireless Devices on District Premises**

1. For security reasons, staff who use their personal device to connect to the Internet, using a District network, will only be permitted to use the District's guest wireless network. Access to any other District network using a personal device is prohibited.
2. Personal devices that have the ability to offer wireless access to other devices must not be used to provide that functionality to others in any District building. The ability to connect personal devices to the District wireless network is a privilege and not a right for employees. Any employee who violates the conditions of this regulation using his/her own device will have his/her access privileges withdrawn.
3. When personal devices are used in District facilities or on the District wireless network, the District reserves the right to:
  - a. Make determinations on whether specific uses of the personally owned wireless devices are consistent with the Employee Acceptable Use of Technology agreement.
  - b. Log network use and monitor storage disk space utilized by such users; and
  - c. Remove or restrict the user's access to the network and suspend the right to use the personally owned computer in District facilities at any time if it is determined that the user is engaged in unauthorized activity, violating the District's Staff Acceptable User of Technology agreement, or violating the terms of this Regulation.

**Sanctions**

The Director of Technology & Communications will report inappropriate behavior to the Superintendent who will take appropriate disciplinary action. Any other reports of inappropriate behavior, violations or complaints will be routed to the employee's supervisor for appropriate action. Violations may result in a loss of access to the DCS and/or disciplinary action. When applicable, law enforcement agencies may be involved.

**SUBJECT: EMPLOYEE USE OF DISTRICT COMPUTER SYSTEM**  
**(Cont'd.)**

**Notification**

All employees will be given access to a copy of the District's policies on staff and student use of computerized information resources and the regulations established in connection with those policies. Any employee who does not receive such documents or needs additional copies of said documents may request them from the District. Each employee will sign an Acceptable Use Agreement before establishing an account or continuing their use of the DCS.

Adopted September 11, 2014

**FREWSBURG CENTRAL SCHOOL DISTRICT  
AGREEMENT USE OF COMPUTERIZED INFORMATION RESOURCES**

In consideration for the use of the Frewsburg Central School District's Computer System (DCS), I agree that I have been provided with a copy of the District's policies on employee and student use of computerized information resources and the regulations established in connection with those policies and I fully understand these policies and regulations and all their provisions. I agree to adhere to the employee policy and the regulations and to any changes or additions later adopted by the District. I shall report all student violations of the District's policy on student use of computerized information resources to my supervisor.

I understand that failure to comply with these policies and accompanying regulations may result in the loss of my access to the DCS and may, in addition, result in the imposition of discipline under the law and/or the applicable collective bargaining agreement. I further understand that the District reserves the right to pursue legal action against me if I willfully, maliciously, or unlawfully damage or destroy property of the District.

Employee Signature \_\_\_\_\_

Date \_\_\_\_\_

School/Building \_\_\_\_\_

**For Office Use Only**

User ID:

Password:

- |  |   |
|--|---|
| <input type="checkbox"/> Database                          | <input type="checkbox"/> Turnitin (7-12)        |
| <input type="checkbox"/> Network                           | <input type="checkbox"/> Castle Learning (K-12) |
| <input type="checkbox"/> Lotus Notes                       | <input type="checkbox"/> Study Island (K-8)     |
| <input type="checkbox"/> Notes Group                       | <input type="checkbox"/> Master Guru (3-5)      |
| <input type="checkbox"/> School World                      | <input type="checkbox"/> ePals                  |
| <input type="checkbox"/> eSchool Data                      | <input type="checkbox"/> Learn360               |
| <input type="checkbox"/> ClearTrack (Spec. Ed.)            | <input type="checkbox"/> Lexia (K-6)            |
| <input type="checkbox"/> Successnet (K-6 all, 7-8 SS only) |   |

## **Frewsburg Central School District Employee Computer Use Agreement**

Every Frewsburg Central School District (hereafter the "District") employee who accesses any aspect of the District's computer system (hereafter "DCS") will be required to read and acknowledge this Computer Use Agreement. **This form supersedes previous forms. Employees who have signed previous forms must also complete this new form.**

Computer use is often a valuable and necessary component of an employee's work. In addition, varying work responsibilities result in access to information sources such as software, programs, the Internet, and the district's computer network. Although employees may have access to these information sources, their use must be specially authorized by the District. Access and authorization to information and equipment carry a corresponding responsibility to their appropriate use. Access should be primarily for educational and professional or career development activities. Electronic mail and telecommunications shall not be utilized to share confidential information about District students, employees, or officials without prior authorization. No employee may disclose, use, or disseminate any personal information regarding District students or employees.

All hardware, including computers and equipment, is the property of Frewsburg Central School District and will fall under the guidelines listed below. Furthermore, all existing District policies, practices, and regulations apply to use of the DCS, especially those that relate to intellectual property protection, misuse of District resources, harassment, bullying, privacy, information security, and confidentiality.

The District's expectations of its employees and staff include, but are not limited to, the following:

1. Student Personal Safety
  - a. Employees who supervise students with access to technical resources shall be familiar with the Frewsburg Central School District Student Internet Safety/Internet Content Filtering Policy (8271) as well as the District Code Of Conduct and enforce its provisions outlines in both documents.
  - b. Student use of technology will be supervised to the extent appropriate. Digital ethics is the responsibility of all who monitor student use..
2. Illegal or Destructive Activities
  - a. Employees will not go beyond their authorized access to the DCS or other computer equipment or software. This will include accessing the files or accounts of others without authorization.
  - b. Employees will not disrupt or attempt to damage or disrupt any technology tools, infrastructure, network capacity, system performance, or data.
  - c. Employees will not use District equipment or personal equipment connected to the District guest network to engage in illegal or offensive acts.
3. System Security
  - a. Employees are responsible for the security of all technology tools, files, and passwords.
  - b. Employees will promptly notify their immediate supervisor or technology department member of security problems.
  - c. Employees with access to student records may not use, release, or share these records (or information contained in these records) except as authorized by Federal and State law.
  - d. Employees whose position and responsibilities require a cell phone or other mobile device for District business purposes and who receive that service through the District service plan must notify the District immediately if their device is lost or stolen. Employees should contact their immediate Supervisor and/or Director of Technology. For District supplied devices, cell and data service will be terminated immediately to protect the organization from unauthorized use.
  - e. Personally owned flash drives shall not be used for District official business purposes.

4. Inappropriate Conduct
  - a. Obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language;
  - b. Potentially damaging, dangerous, or disruptive material;
  - c. Racial, sexual or other harassment of bullying in violation of District policies or regulations; and
  - d. False or defamatory information.
5. Plagiarism and Copyright Infringement
  - a. Works may not be plagiarized.
  - b. The rights of copyright owners are to be respected. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by copyright. If an employee is unsure whether or not a work can be used, the copyright owner should be contacted to request his or her permission to use the work. No work shall be used without the express written consent of the copyright owner.
  - c. Software copyrights and software licenses must be strictly respected.
6. Inappropriate Access to Material
  - a. Technology resources will not be used to access or disseminate material that is profane, obscene (pornographic), or advocates illegal acts, violence, or illegal discrimination. Inadvertent inappropriate access will be reported immediately to the supervisor.
  - b. The use of Internet games, web chats, unauthorized software, or non-authorized instant messaging software (e.g. AOL Instant Messenger, etc.) is prohibited. except when specifically authorized by the District Superintendent or a person of his/her designee.
  - c. Use of publicly available non-District created Web collaboration tools such as blogs, wikis and social networking tools for work purposes is acceptable, if conducted in accordance with Regulation #6471R – Social Media Guidelines for Employees. Employees must use District authorized resources to create teacher or classroom web pages. Unofficial personal use of social networking sites or Web 2.0 collaboration tools during the work day using District technology resources is not permitted without prior supervisor approval initiated by an employee's supervisor. Excessive use of personal technology devices for non-work related activity during the work day is not permitted and may result in disciplinary action.
7. Expectation of Privacy

Employees have no expectation of privacy in files, disks, hardware, or documents that have been created in, entered in, stored in, downloaded from, or used on District equipment.
8. Services and Assumption of Risks

Frewsburg Central School District makes no warranties of any kind, whether express or implied, for services provided and is not responsible for any damages suffered while on the system to including, but not limited to, loss of data and inaccurate or poor quality information obtained via the DCS. Users are responsible for backing up data stored locally on any device assigned to them.
9. Discipline
  - a. Employees who engage in unacceptable use may lose access to technology tools provided by the District and may be subject to further discipline in accordance with applicable law and collective bargaining agreements.
  - b. Deliberate violations of this agreement (e.g., malicious acts or omissions; searching for, viewing or otherwise visiting pornography or sexually explicit sites) are cause for disciplinary action up to and including termination.

10. Unacceptable Uses

- a. Illegal or malicious use, including downloading or transmitting of copyrighted material such as music, videos and games.
- b. To solicit personal information with the intent of using such information to cause emotional or physical harm.
- c. Downloading of music, games or other programs, or streaming of music or video for personal use are prohibited.
- d. To disrupt the work of other users. This included the propagation of computer viruses and use of the Internet to make unauthorized entry to any other Internet resource.
- e. Use for private business purposes. This includes, but is not limited to, the installation or loading of personal business programs onto your computer for your use for tasks not associated with your Frewsburg Central School District job duties.
- f. Excessive personal use of Internet or e-mail, during the work day, may result in disciplinary action.

11. E-Mail

- a. Every user is responsible for all e-mail originating from their user ID e-mail address. Forgery or attempted forgery of electronic mail is prohibited. The District's e-mail standard (currently, Domino Lotus Notes) is the only allowable e-mail to be used. Do not access your personal e-mail account (ex. Hotmail, AOL, etc.) through the DCS.
- b. Attempts to read, delete, copy, or modify the e-mail of other users are prohibited.
- c. E-mail is NOT private. The District Superintendent (or designee) has the right of access to all e-mail sent or received. In the event of Frewsburg Central School District being involved in any legal proceedings, any relevant e-mails (including Internet e-mail) may have to be disclosed, on the same basis as the case for written documents.
- d. Forwarding of chain letters is not allowed.

I have read the Employee Computer Use Agreement and received the *Computer Guidelines and Rules*. I understand that failure to comply with these policies and accompanying regulations may result in the loss of my access to the DCS and may, in addition, result in the imposition of discipline under the law and/or the applicable collective bargaining agreement. I further understand that the District reserves the right to pursue legal action against me if I willfully, maliciously or unlawfully damage or destroy property of the District.

PLEASE PRINT

FIRST NAME \_\_\_\_\_ LAST NAME \_\_\_\_\_

DEPARTMENT/PROGRAM \_\_\_\_\_

BUILDING \_\_\_\_\_

SIGNATURE \_\_\_\_\_ DATE \_\_\_\_\_

# ***Frewsburg Central School District***

## ***Computer Guidelines & Rules***

### ***District policies are in place for the following purposes:***

1. Uphold and comply with all Federal & State laws
2. Provide appropriate safeguards for our students
3. Protect the District and employees from liability
4. Keep losses in terms of equipment, software, and time required for repairs to a minimum.
5. Ensure problems are resolved in a timely manner.

### ***Federal & State Laws regarding Technology***

Computer Technology in schools has empowered users to create professional looking documents. With this, there is a greater potential for document fraud. In some cases, copying ALONE is illegal with or without intent to use or profit from the fraudulent documents.

### ***Federal laws prohibit copying the following:***

**It is illegal to reproduce currency in any form.**

Any form of copying is illegal. This includes photocopying, scanning, or any electronic format of currency. It does NOT matter how obviously "fake" the copy is, even black & white, resized, or altered in appearance. It does not matter what the copier's intent was. It does not matter what age the copier is.

---

**It is illegal to reproduce ID and other Federal security documents such as a passport, Certificate of Citizenship, Certificate of Naturalization, Social Security cards, or Permanent Residence cards.**

Violation of these Federal laws will result in a minimum penalty of 5 years in Federal penitentiary plus severe monetary fines.

---

**It is illegal to reproduce and/or alter other State or County government issued ID documents such as driver's license, Sheriff's ID, etc.**

Violations are under State laws and penalties range from fines to confinement.

---

**It is illegal to reproduce copyrighted documents.  
It is illegal to reproduce patented materials.**

Federal Copyright Laws and US Patent Laws are in place to protect the intellectual work of others. This includes published or unpublished writing, music, art, audio recordings, video, and other electronic works such as webpages. Refer to the handout on Copyright for more details on copyright. Patent Laws in general cover objects, devices, and plans for devices.

---

**Fair Use exemption to copyright law is in place to allow commentary, news reporting, parody, research, and education about copyrighted works without the permission of the author.**

This law allows educators to use excerpts of works for study. It does not allow teachers to copy indiscriminately. When in doubt, contact your library media specialist or the technology department.

## *Federal Laws related to Software -*

<b>Only software purchased by the district will be installed on district computers.</b>	Ensures the District is in legal compliance with Federal software licensing laws.
<b>Only Technology Services personnel will install software.</b>	Tech Services is responsible for software licensing and this restriction ensures legal compliance.
<b>Security software is installed on computers to prevent users from installing, deleting software or modifying system settings.</b>	Assurance of Legal compliance Also reduces computer problems requiring tech support resulting from improper system settings or missing software or files.

## *Email & other communications-*

<b>It is illegal to use email or any communications for threats or extortion.</b>	TITLE 18: CHAPTER 41 - EXTORTION AND THREATS / 871. Threats against President and successors to the Presidency. / 872. Extortion by officers or employees of the United States. / 873. Blackmail. / 874. Kickbacks from public works employees. / 875. Interstate communications. / 876. Mailing threatening communications. / 877. Mailing threatening communications from foreign country. / 878. Threats and extortion against foreign officials, official guests, or internationally protected persons. / 879. Threats against former Presidents and certain other persons protected by the Secret Service. / 880. Receiving the proceeds of extortion.
<b>It is illegal [to use email] to harass, defame, or sexually harass others.</b>	Additionally, current legislation is pending concerning Cyber-stalking.
<b>The District provides email accounts on a limited basis to students or non-District personnel.</b>	Refer to the next section on CIPA and the section on Email.

## *The Children's Internet Protection Act (CIPA)*

Recent federal laws require school compliance with CIPA regulations regarding student safety and internet access. The Children's Internet Protection Act (CIPA) was signed into law on December 21, 2000 and became effective April 20<sup>th</sup>, 2001. Pursuant to the Children's Internet Protection Act, as codified at 47 U.S.C. / 254(h) and (l), school districts must certify the following with regard to electronic mail.

The Internet Safety Policy must address the following issues:

- a. access by minors to inappropriate matter on the Internet and World Wide Web;
- b. the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- c. unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- d. unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- e. measures designed to restrict minors' access to materials harmful to minors.

**The District ensures compliance** with this portion of CIPA by the following:

1. Email accounts will be provided to students at Frewsburg Central schools on a limited basis. Email use by students for a specific class project may be done ONLY under direct teacher supervision with authorization from Technology Department. Only COPPA and CIPA compliant mail accounts, which have content filtering and address control will be used by students. The teacher will be responsible for reviewing all messages deemed questionable by the filter. The teacher also must ensure that a student

does not unwittingly reveal personal information or receive any incoming email from an unauthorized source that would be deemed harmful to a minor.

2. Access to the Internet through the Frewsburg Central School District computer network from any computer is protected through Internet filtering software. With the ever changing Internet, no filtering software is 100% effective, therefore it is imperative to always monitor students while they are on the Internet.

3. Unauthorized disclosure of information is a District policy in compliance also with FERPA regulations.

## ***Protecting Children in the 21st Century Act***

School E-Rate recipients will be required to certify that they are “educating minors about appropriate online behavior, including interacting with other individuals on social networking Web sites and in chat rooms as well as cyberbullying awareness and response”.

## ***District Policies and Procedures***

### ***Integrity of Network Data and District Information Systems***

The reliability and integrity of the network is dependent on the care of those who use it. Protecting all passwords and access to various network data are important. All faculty and staff are to be particularly vigilant in securing their login and passwords, signing on and off the system. Much of the information faculty and staff have access to is confidential and Federal laws regulate the release of such information, all staff are responsible for the following:

1. Securing your login name and password so it is inaccessible to all others. NEVER give out your password or those of other staff to anyone.
2. Logging out completely when finished. Do not leave your system logged in if you will not be in the room.
3. Ensuring that confidential data cannot be viewed or accessed by students, parents, or others.
4. Non-Disclosure of information: Federal laws under the **Family Privacy Act** prohibit school personnel from releasing certain information about a student or student's family. If an individual requests information, you are to direct them to the principal's office & follow-up by contacting the principal and alerting them of the request. (Recruiters, photographers, salespersons and individuals with their own private agenda seek lists of students, telephone numbers, etc.)

### ***General Network Policies***

No one is to enter or have access to network resources without authorization.

---

No one is to tamper with or destroy computer data or files that do not belong to him or her.

---

No one is to distribute access codes, passwords or otherwise provide the means for any unauthorized person to use the network.

### ***Equipment –***

No personally owned computer or video equipment is to be brought into school for classroom use without prior consent.

---

No one is to attach any computer or other equipment to the network unless authorized by the District Technology Coordinator or District Technician.

---

---

No one is to detach or move computers from the network or move computers from their designated location unless authorized by the District Technology Coordinator or District Technician.

---

Physical modifications to district equipment, including but not limited to removing logic boards, memory modules, drives, cables is expressly prohibited.

---

### *Software & Videotape –*

Only software purchased by the District will be loaded on District computers.

---

Individuals will not load personally acquired software on the computers or network, unless authorized by the District Technology Coordinator or District Technician.

---

All requests for software purchase will be evaluated within the guidelines of selecting other instructional material, giving care to avoid inappropriate or biased material.

---

Building Principals will be responsible for collecting suggestions and requests as part of the requisition process. The technology department will evaluate all software requests for compatibility with the district computer system.

---

### *E-Mail –*

E-Mail is provided to District Staff to improve communications within the district and to empower staff to obtain information related to their assignment that would otherwise be unavailable. No one is to provide another user's email address to others without the owner's express consent.

---

Use of Email for personal gain, commercial purposes, illegal activities, or to violate Federal and/or State laws is expressly forbidden.

---

No one is to use Email to distribute abusive, harassing, libelous, obscene, offensive, profane, pornographic, threatening, sexually explicit, or any other illegal material.

---

### *Purchasing of Software & Hardware –*

All grant proposals which are requesting or applying for technology-related items [including but not limited to staff development or training, computer hardware, software, networking components or network software, computer peripherals such as scanners, printers, projection devices, digital cameras, and digital video cameras] must be developed in partnership with the District Technology Coordinator.

---

Grant proposals which have not met this requirement will not be sanctioned by Administration.

---

Donated equipment must meet district standards and must be approved by the District Computer Technician before acceptance.

---

### *Requests for Technology Support –*

Requests for hardware assistance or technical support are to be submitted to Technology Department through the tech help form. This can be accessed via the Tech Support button on the district's email Welcome Page or through the following link: <http://www.frewsburgcsd.org/intranet/TechHelp.cfm> This account is monitored on a regular basis and calls are prioritized by the technology department staff. Phone calls, emails, or other impromptu requests that are **not** submitted through the tech help form will not be addressed.

---

Hardware & technical support is provided for district purchased equipment only.

---

---

Software assistance and instructional support questions are to be directed to the District. Software support and training for teachers and staff is provided for those software titles purchased by the District.

---

Requests for software support or instructional assistance should be forwarded to the District Technology Coordinator, not other administrators, other buildings or departments, or individuals outside the District. Requests for software assistance can be sent through the Tech Help (Tech Support) link.

### *Classroom WebPages –*

The District maintains a website that provides all teachers the opportunity to post a classroom webpage. Teachers are strongly recommended to keep these web pages current with contact information and pertinent class information. This is one way to maintain communication with parents/guardians.

---

Teachers and staff are not to post school-related web pages on an independent domain. Additionally, they are not to post any school or student related information on the Internet without express authorization from the Superintendent.

---

Consequences for infractions of the District's policies regarding computer usage may result in suspension or termination of the website, loss of access privileges and/or appropriate disciplinary action. Activities in violation of state and/or federal statutes will be subject to prosecution by those authorities. Additional disciplinary action may be taken as deemed appropriate by the District for the specific violation.

*Modified and presented with permission from Susan Ciminelli, Lakeshore District Technology Coordinator*