Brasher Falls Central School District
St. Lawrence Central School

PO Box 307
Brasher Falls, New York 13613
(315) 389-5131
(315) 389-5245 Fax

Acceptable Use Policy

The Policy

The Brasher Falls Central School District provides access to the District's Internet Systems for its employees, agents, students, and volunteers, collectively referred to as "users" for educational and business purposes, in conformance with applicable law. This Internet Acceptable Use and Safety Policy ("policy") governs all electronic activity of users using and accessing the District's Internet systems, including District e-mail and District-provided access to the Internet, and applies to the use of the District Internet Systems both on and off District property.

"The District's Internet Systems" means District-provided devices, Internet connections (including wireless connections) provided by the District, District-provided e-mail accounts, intranet and any remote connection to District systems. A user is deemed to access and use the District's Internet Systems through any electronic activity conducted on the District's Internet Systems using any device (whether or not such device is a District-provided device) regardless of the user's physical location.

"District-provided devices" means any electronic device provided by the District, including, but not limited to, desktop computers, laptops, Chromebooks, and hand-held devices, such as personal digital assistants (PDAs), smartphones, iPads, tablets and e-readers.

Student use of the District's Internet Systems is governed by this policy, District regulations, policies and guidelines, and applicable law. Employee use is governed by this policy, District regulations, policies and guidelines, the District's employment policies, applicable collective bargaining agreements, and applicable law.

By using the District's Internet Systems, a user agrees to follow this policy and all applicable District regulations, policies and guidelines. All users must report any misuse of the network or Internet or receipt of any communication that violates this policy to a teacher, supervisor or other appropriate District personnel.

Principles of Acceptable and Safe Internet Use

General

Internet access and e-mail provided by the District are intended for educational use, instruction, research and the facilitation of communication, collaboration, and other District related purposes. Users are subject to the same standards expected in a classroom and/or professional workplace.

Monitoring and Privacy

Users have no right to privacy while using the District's Internet Systems. The District monitors users' online activities and reserves the right to access, review, copy, store, or delete any electronic communications or files. This includes any items stored on District-provided devices, such as files, e-mails, cookies, and Internet history.

The District reserves the right to disclose any electronic activity, including electronic communications, to law enforcement officials or third parties, as appropriate and consistent with applicable law. The District will fully cooperate with local, state, or federal officials in any lawful investigation concerning or relating to any illegal activities conducted through the District's Internet Systems.

Prohibited Uses of the District's Internet Systems

Users may not engage in any of the activities prohibited by this policy when using or accessing the District's Internet Systems.

If a user is uncertain whether behavior is prohibited, he or she should contact a teacher, supervisor or other appropriate District personnel. The District reserves the right to take immediate action regarding activities that (1) create security and/or safety issues for the District, students, employees, schools, network or computer resources, or (2) expend District resources on content the District determines lacks legitimate educational or District content or purpose, or (3) the District determines are inappropriate.

Below is a non-exhaustive list of examples of prohibited behavior:

1. Causing harm to others, damage to their property or District property, such as:

    - Using, posting or distributing profane, lewd, vulgar, threatening, or abusive language in e-mail messages, chat rooms, or instant messages, material posted on District web pages, or professional social media sites;
    - Accessing, using, posting, or distributing information or materials that are pornographic or otherwise obscene, advocate illegal or dangerous acts, or advocate violence or discrimination. If users inadvertently access such information, they should immediately disclose the inadvertent access in a manner specified by their school or central division office;
    - Accessing, posting or distributing harassing, discriminatory, inflammatory, or hateful material, or making damaging or false statements about others;
    - Sending, posting, or otherwise distributing chain letters or engaging in spamming;
    - Damaging computer equipment, files, data or the District's Internet System in any way, including spreading computer viruses, vandalizing data, software or equipment, damaging or disabling others' electronic property, or engaging in conduct that could interfere or cause a danger of disruption to the District's educational or business environment;
    - Using the District's Internet System in a manner that interferes with the education of the user or others or the job duties of the user or others;
    - Downloading, posting, reproducing or distributing music, photographs, video or other works in violation of applicable copyright laws. Any music, photographs and/or video should only be downloaded for District, and not personal purposes. If a work specifies how that work may be used, the user should follow the expressed requirements. If users are unsure whether or not they can use a work, they should request permission from the copyright or trademark owner; or
    - Engaging in plagiarism. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.

2. Gaining or attempting to gain unauthorized access to the District's Internet Systems, or to any third party's computer system, such as but not limited to:

    - Malicious tampering, phishing or hacking activities;

- Intentionally seeking information about passwords belonging to other users;
- Disclosing a user's password to the District's Internet Systems to other individuals. However, students may share their District password with their parents.
- Modifying passwords belonging to other users;
- Attempting to log in through another person's account;
- Attempting to gain access to material that is blocked or filtered by the District;
- Accessing, copying, or modifying another user's files without authorization;
- Disguising a user's identity;
- Using the password or identifier of an account that does not belong to the user; or
- Engaging in uses that jeopardize access into others' accounts or other computer networks.

3. Using the District's Internet Systems for commercial purposes, such as:

    - Using the District's Internet Systems for personal financial gain;
    - Conducting for-profit business activities, personal advertising, or other non-District business communications;
    - Using the District's Internet Systems on behalf of any elected official, candidate, candidates, slate of candidates or a political organization or committee.

4. Engaging in criminal or other unlawful activities.

Filtering

In accordance to Children's Internet Protection Act ("CIPA"), the District blocks or filters content over the Internet that the District considers inappropriate for minors. This includes pornography, obscene material, and other material that may be harmful to minors. The District may also block or filter other content deemed to be inappropriate, lacking educational or work-related content or that pose a threat to the network. The District may, in its discretion, disable such filtering for certain users for bona-fide research or other lawful educational or business purposes.

Users shall not use any website, application, or methods to bypass filtering of the network or perform any other unlawful activities.

Protection of Personally Identifiable & Confidential Information

The Family Educational Rights and Privacy Act ("FERPA") prohibits District school officials from disclosing personally identifiable information ("PII") from education records of District students and families to third parties without parental consent. However, several exceptions to this general rule may apply.

All users of the District's Internet Systems must comply with FERPA and Confidentiality and Release of Student Records; Records Retention. If you are unsure about whether the activity will comply with, please contact a member of the District's administrative staff.

Student Internet Safety

1. District Responsibilities:

    - The District will provide curriculum about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

- The District will work to protect the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
- As appropriate, the District will provide students, staff and parents with guidelines and instructions for student safety while using the Internet.

2. Students Using the District's Internet Systems

- Students must not reveal personal information about themselves or other persons on social networking sites, in chat rooms, in emails or other direct electronic communications, or any other forum over the Internet. For example, students must not reveal their home address, or telephone or cell phone number. Students must not display photographs of themselves, or the images of others.
- Students should not meet in person anyone they have met only on the Internet.
- Students must promptly disclose to their teacher or other school employee any message or other activity they receive that is inappropriate or makes them feel uncomfortable.
- Students should not allow District computers to save their passwords.

3. Teachers and Faculty using the District Internet Systems, including Social Media for class activities

- Teachers should educate students about appropriate and safe online behavior, including interacting with individuals on social networking websites and in chat rooms and cyberbullying awareness and response. Teachers should refer to the following guide at http://goo.gl/SRpR9N and other free educational Internet safety resources available on the Internet.
- Social Media
    - "Social media" means any form of online publication or presence that allows interactive communication, including, but not limited to, social networks, blogs, Internet websites, internet forums, and wikis. Examples of social media include, but are not limited to, Facebook, Twitter, YouTube, Instagram, Snapchat, Google+, and Flickr.
    - Schools use a variety of online web-based interactive communication technologies to enhance students' education and learning. Social media sites must be used only for educational and school related purposes, in connection with lessons and assignments and to facilitate communication with teachers and other students.
    - The District limits access to these sites to individuals within the District and District school officials. If access to a social media site will extend beyond individuals within the District or District school officials, then parent consent is required.

4. Parents:

- Although students generally will be supervised when using the District's Internet System on school property, it is not practicable for the District to monitor and enforce a wide range of social values in student use of the Internet. Parents are primarily responsible for transmitting their particular set of family values to their children, and discussing with their children what material is and is not acceptable for their children to access through the District's Internet Systems.
- Parents are exclusively responsible for monitoring their children's use of the Internet when the District's Internet Systems are accessed from home or a non-school location. The District may or may not employ its filtering systems to screen home access to the District's Internet Systems. Parents should inquire with the school or District.

Violations of this Policy

The District, including central offices and schools, reserves the right to terminate any user's access to District Internet Systems - including access to District e-mail - at any time.

If a student violates this policy, appropriate disciplinary action will be taken consistent with the Discipline Code. If a student's access to the District's Internet System is revoked, the student may not be penalized academically, and the District will ensure that the student continues to have a meaningful opportunity to participate in the educational program.

Employee violations of this policy will be handled by appropriate discipline.

All users must promptly disclose to their teacher, supervisor, principal or manager any information they receive that is inappropriate or makes them feel uncomfortable.

Limitation of Liability

The District makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the District’s network are to be borne by the user. The District also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the District, its affiliates, or employees.

Office Use Only:

Username:

_____

Password:

_____

STUDENT USER AGREEMENT AND PARENT PERMISSION FORM

This form must be completely filled out for your network and email accounts to be activated. If you don't know how to respond to any item, please ask for assistance.

PLEASE PRINT: Illegible responses will be considered incomplete.
This form is to be completed by all students in the district and will be kept on file in the main office.

Student LAST Name: _____

Student FIRST Name: _____

Year of Graduation: 20__ __ Date of Birth: ___ / ___ / ___ Home Phone: _ _ _ - _ _ _ _

Student ID Number: __ __ __ ___ Homeroom Teacher or #: _____

Desired Password (at least 8 characters, at least one #): _____

☛***Student:*** ***Please read and sign below. Return this full page to your homeroom teacher.***

As a user of the Brasher Falls Central School computer network, I have read and hereby agree to comply with the Computer Use Policy located in the student handbook. I understand that network privileges can and will be suspended or revoked if I fail to fully comply. I understand that I am not to share my UN or PW with others.

STUDENT SIGNATURE: _____ Date: _____

☛***Parent:*** ***Please read and sign below. This form must be returned to your child's homeroom teacher.***

As a parent or guardian of a Brasher Falls Central School student, I have read the Computer Use Policy located in the student handbook regarding student use of the computer network. I have discussed the rules and procedures with my son/daughter and agree to allow him/her to utilize the districts email and network systems, and the Internet as long as he/she upholds those rules. I understand that computer network privileges can and will be suspended or revoked for a student who does not comply.

PARENT SIGNATURE: _____ Date: _____