Brasher Falls Central School

Computer/Chromebook Use Program

2026-2027

St. Lawrence Central School
1039 State Highway 11C
P.O. Box 307
Brasher Falls, NY 13613
Phone: 315-389-5131
Fax: 315-389-5245

Updated July 30, 2026

Brasher Falls Central School District
Computer/Chromebook Use Program

The focus of the Brasher Falls Central School District Computer Use Program is to prepare students for their future, a world of digital technology and information. An atmosphere that provides students with immediate access to online resources, local network resources, online-based information, and textbooks is essential to thrive in the 21st century. Research indicates that students who have access to technology on a regular basis show a significant improvement in their learning skills over those who do not have this opportunity. With this in mind, every effort will be made to provide access to quality resources that will reshape how students learn.

With the provision of school-based computing devices comes the need to establish rules, policies, and regulations that will govern the use of the equipment. These issues range from the need to protect student access to care and maintenance of the devices. Each student in grades K-12 will have access to school-provided computers during the school day. Devices are provided for use in school only and remain the property of Brasher Falls Central School District at all times.

Students live in an on-demand, technology-dependent world. They learn differently and approach school work differently than students did even a few years ago. Excellence in education requires that technology is seamlessly integrated throughout the educational program. Increasing access to technology is essential for that future. The use of school-provided computers/Chromebooks is a way to empower students to learn at their full potential and to prepare them for the real world of college and the workplace. Computers encourage students to solve problems and think critically by stimulating analytical thinking. Learning results from the continuous dynamic interaction among students, educators, parents, and the extended community. Technology immersion does not diminish the vital role of the teacher. To the contrary, it transforms the teacher from a director of learning to a facilitator of learning. The computer/Chromebook program integrates technology into the curriculum anytime during the school day.

Establishing this new environment for such learning takes careful planning and consideration. We hope the information in this guidebook provides you with useful information, advice, best practices, and practical solutions. This guidebook is not meant to be "all inclusive" and will remain a work in progress as the computer/Chromebook use program develops over the years. While the success of any program of this magnitude depends on individual goals, school-wide goals, environments, planning, and personnel – certain strategies can be universal. The keys to our goal and objective-setting process will focus on enhancing student learning while aligning our technology and instructional policies.

The policies, procedures, and information within this document apply to all computers/Chromebooks and devices used at Brasher Falls Central School District, including any other device considered by administration to come under this policy. Teachers may set additional requirements for computer/Chromebook use in their classroom.

---

1. ACCESSING COMPUTERS AT SCHOOL

School-provided computers/Chromebooks will be available for student use during the school day as directed by teachers and staff. Parents and students must sign and return the Student Contract for Computer Use document before the student can access school computers. Computers/Chromebook will be maintained throughout the school year for updates, cleaning, and software installations.

---

2. TAKING CARE OF YOUR SCHOOL COMPUTER

Students are responsible for the proper care of school-provided computers/Chromebooks while they are using them during the school day. Computers/Chromebooks that are broken or fail to work properly must be reported to the Technology Department located in the Middle School Technology Office.

2.1 General Precautions

- No food or drink is allowed next to your computer/Chromebook while it is in use.
- Cords, cables, and removable storage devices must be inserted carefully into the computer/Chromebook.
- Computers/Chromebooks must remain free of any writing, drawing, etching, etc.
- Computers/Chromebooks must never be left in an unsupervised area.
- No stickers may be placed on school computers/Chromebooks

2.2 Carrying Computers

- Computers/Chromebooks should always be within the protective case when carried.
- Some carrying cases can hold other objects (such as folders and workbooks), but these must be kept to a minimum to avoid placing too much pressure and weight on the computer.

2.3 Screen Care

- Computer/Chromebook screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure.
- Do not lean on the top of the computer/Chromebook when it is closed.
- Do not place anything near the computer/Chromebook that could put pressure on the screen.
- Do not place anything in the carrying case that will press against the cover.
- Do not poke the screen.
- Do not place anything on the keyboard before closing the lid (e.g. pens, pencils, or disks).
- Clean the screen with a soft, dry cloth or anti-static cloth.

---

3. USING YOUR COMPUTER/CHROMEBOOK AT SCHOOL

Computers/Chromebook are intended for educational use at school during the school day. School messages, announcements, calendars, and schedules can be accessed using the computer. Students must follow teacher directions regarding computer/Chromebook use in each classroom.

3.1 Computers/Chromebooks Undergoing Repair

If a computer/Chromebook needs repair, a replacement device may be provided for classroom use while repairs are completed.

3.2 Sound

Sound must be muted at all times or headphones/earbuds must be used in the classroom, unless permission is obtained from the teacher for instructional purposes.

3.3 Printing

Students may use the printers located in the Library or Computer lab around the school with teachers' permission during class or breaks.

3.4 Screensavers & Backgrounds

Inappropriate media may not be used as a screensaver or background. Presence of guns, weapons, pornography, inappropriate language, alcohol, drug, gang related symbols or pictures will result in disciplinary actions.

3.5 Music & Games

Music and games are not allowed to be used on school computers/Chromebooks during school hours.

---

4. MANAGING YOUR FILES & SAVING YOUR WORK

4.1 Saving to the Cloud

All student work will be saved on the BFCSD assigned Gmail account on their Google Drive. The student is responsible for managing and not sharing usernames and passwords for any school related accounts. Students are responsible for ALL actions that occur on their BFCSD accounts.

---

5. ACCEPTABLE USE

5.1 General Guidelines

- Access to the district's computer network is provided for educational purposes and research consistent with the district's mission and goals.
- Use of the district's computer network is a privilege, not a right. Inappropriate use may result in disciplinary consequences consistent with the student Code of Conduct.
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- All network users have been issued a login name and password which are not to be shared with others. Passwords must be changed periodically. Students who have knowledge of another person's access information shall report it to the building principal.
- All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive or sexual language or images, vulgarities and swear words are all inappropriate.
- Network users identifying a security problem on the district's network must notify the appropriate teacher, administrator, or computer network coordinator. Under no circumstance should the user demonstrate the problem to anyone other than to the district official or employee being notified.
- Any network user identified as a security risk or having a history of violations of district computer use guidelines may be denied access to the district's network.

5.2 Prohibited Activity & Uses

The following is a list of prohibited activity concerning use of the district's computer network. Violation of any of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the network.

- Using the network for commercial activity, including advertising.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting, or making available any copyrighted software on the district computer network.
- Using the network to receive, transmit, or make available to others obscene, offensive, or sexually explicit material.
- Using the network to receive, transmit, or make available to others messages that are racist, sexist, abusive, or harassing to others.
- Using another user's account or password.
- Attempting to read, delete, copy, or modify the electronic mail (e-mail) of other system users and deliberately interfering with the ability of other system users to send and/or receive email.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy district equipment or materials, data of another user of the district's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network.
- Using the network to send anonymous messages or files.
- Using the network to receive, transmit, or make available to others a message that is inconsistent with the district's Code of Conduct.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software or using personal disks on the district's computers and/or network without the permission of the appropriate district official or employee.
- Using district computing resources for commercial or financial gain or fraud.
- Stealing data, equipment, or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, or vandalize the data of another user.
- Changing or exceeding resource quotas as set by the district without the permission of the appropriate district official or employee.
- Using the network while access privileges are suspended or revoked.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

5.3 No Privacy Guarantee

Students using the district's computer network should not expect, nor does the district guarantee privacy for electronic mail (e-mail) or any use of the district's computer network. The district reserves the right, upon reasonable cause for suspicion, to access all aspects of its computing and network resources, including individual usage to determine if a user is violating this policy or state or federal laws.

5.4 Sanctions

All users of the district's computer network and equipment are required to comply with the district's policy and regulations governing the district's computer network. Failure to comply with the policy or regulation may result in disciplinary action consistent with the student Code of Conduct.

In addition, illegal activities are strictly prohibited. Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state, and/or local law or regulation is prohibited. This includes, but is not limited to materials protected by copyright, threatening or obscene material, or material protected by trade secret. Users must respect all intellectual and property rights and laws.

5.5 District Responsibilities

The district makes no warranties of any kind, either expressed or implied, for the access being provided. Further, the district assumes no responsibility for the quality, availability, accuracy, nature, or reliability of the service and/or information provided. Users of the district's computer network and the Internet use information at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided.

The district will not be responsible for any damages suffered by any user, including, but is not limited to, loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by its own negligence or the errors or omissions of any user. The district also will not be responsible for unauthorized financial obligations resulting from the use of or access to the district's computer network or the Internet.

Further, even though the district may use technical or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the district policy and regulation.

5.6 Student Responsibilities

- Students may only log in under their own username. Students may not share their password with other students.
- Students must follow all teacher directions regarding computer use.
- All use of the Internet must comply with district guidelines. Log files are maintained on each computer with a detailed history of all sites accessed. These files will be reviewed periodically.

5.7Parental Responsibility

- Parents will be responsible for reviewing the Acceptable Use Policy with their child(ren)/student(s).

---

6. PROTECTING SCHOOL COMPUTERS/CHROMEBOOKS

6.1 Computer/Chromebooks Identification

School computers will be labeled in the manner specified by the school. Computers/Chromebooks can be identified in the following ways:

- Record of serial number and district asset tag
- Individual User account name and password
- Monitoring/Tracking Software

6.2 Password Protection

Students will be given a password to access cloud-based district resources. Students are expected to keep their passwords confidential.

6.3 Storing Computers/CHROMEBOOKS

When students are not using computers, they will be stored securely by school staff. Computers/Chromebooks should never be stored in student lockers or vehicles. Computers/Chromebooks remain under school supervision at all times.

6.4 Computers/CHROMEBOOKS Left in Unsupervised Areas

Under no circumstances should computers/Chromebooks be left in unsupervised areas. Unsupervised areas include the school grounds and campus, the cafeteria, computer lab, locker rooms, unlocked classrooms, and hallways. Any computer left in these areas is in danger of being stolen. Unsupervised computers/Chromebooks will be collected by staff and taken to the

Technology Department. Disciplinary action may be taken for leaving a computer/Chromebook in an unsupervised location.

---

7. REPAIRING OR REPLACING SCHOOL COMPUTERS/CHROMEBOOKS

In the event that a school computer/Chromebook is not operating correctly or is damaged, please report it to the Technology Department as soon as possible. A replacement device may be provided for classroom use while repairs are completed.

INTENTIONAL DAMAGE: Students/Parents are responsible for full payment of intentional damages to computers/Chromebook or accessories (bags, chargers, etc.). Warranty DOES NOT cover intentional damage of the computer.

---

8. COMPUTER/CHROMEBOOK TECHNICAL SUPPORT

The Technology Department is located in room 202 and coordinates the support for school computers. Services provided include the following:

- Hardware maintenance and repairs
- Password identification
- User account support
- Operating system or software configuration support
- Application information
- Updates and software installations
- Coordination of warranty repairs
- Distribution of replacement devices and batteries

---

9. COMPUTER/CHROMEBOOK USE PRIVILEGES SYSTEM

All students will begin the school year with Standard Privileges. Student records will be reviewed quarterly to determine whether they have earned the opportunity to keep all standard privileges.

Description of Privileges & Criteria

Standard Privileges:

- Computer/Chromebook use at school
- Gmail account for student information

Standard Privileges Criteria

Students will begin on this level at the beginning of the school year. To remain at this level, students will have:

- Less than 2 incidents of accidental damage
- No more than 1 incident of a computer violation
- No incidents of Computer Network Violations

Suspended Privileges:

- Computer/Chromebook use at school may be restricted
- Gmail account for student information may be restricted

Suspended Privileges Criteria

Students will be placed at this level if they have:

- Two or more incidents of accidental damage
- Two or more incidents of Computer Violations
- One or more incidents of Computer Network Violation

---

10. Use of Technology Resources Policy

Purpose

The Brasher Falls Central School District is pleased to offer students, faculty, and staff access to technology resources for schoolwork and enrichment activities. The purpose of the Brasher Falls Central School District's technology resources is to provide additional educational resources and communication tools for students and teachers. These resources will help teachers to facilitate education and research consistent with the objectives of the Brasher Falls Central School District.

Definition – Technology Resources

The Brasher Falls Central School District's technology resources include but are not limited to the following resources: network, Internet, computer hardware, software, printers, servers, stored text, data files, electronic mail, optical media, digital images, and new technologies as they become available.

Regulations

The use of the Brasher Falls Central School District's technology resources is a privilege, not a right. The privilege of using the technology resources provided by the school district is not transferable or extendible by students to people or groups outside the district and terminates when a student is no longer enrolled in the Brasher Falls Central School District. This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the User Terms and Conditions named in this policy, privileges may be terminated, access to the school district technology resources may be denied, and the appropriate disciplinary action shall be applied. The Brasher Falls Central School District's Code of Conduct shall be applied to student infractions.

User Terms and Conditions

Use of Brasher Falls Central School District's technology is subject to the following terms and conditions:

The use of technology resources must be for educational and/or research purposes consistent with the mission, goals, and objectives of the Brasher Falls Central School District along with State and Federal regulations. In compliance with federal law, the school district shall make reasonable effort to restrict access to inappropriate materials and shall monitor the online activities of the end users in the school environment.

User accounts are considered the property of the school district. Network administrators may review school computers to maintain system integrity and to ensure that users are using the

system responsibly. While user files will not be examined without reasonable cause, users should not expect that anything stored on school computers or networks will be private.

1. Prohibited technology resources activities include, but are not limited to, the following:

   Chromebook/Computer Violations:
   - Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials.
   - Downloading or transmitting multiplayer game, music, or video files using the school network.
   - Vandalizing, damaging, or disabling property of the school or another individual or organization.
   - Accessing another individual's materials, information, or files without permission.
   - Using the network or Internet for commercial, political campaign, or financial gain purposes.
   - Releasing files, home address, personal phone numbers, passwords, or other vital information to others.
   - Promoting or soliciting for illegal activities.
   - Attempting to repair, remove or install hardware components.
   - Violating copyright or other protected material laws.
   - Subscribing to mailing lists, mass email messages, games, or other services that generate several messages that can slow the system and waste other users' time and access.
   - Intentionally wasting school resources.

   Consequences:
   - 1st offense – Office intervention or 5 day chromebook suspension
   - 2nd offense – 10 day chromebook suspension
   - 3rd offense – Chromebook suspended for remainder of quarter or not less than 10 days.

   Computer Network Violations:
   - Attempting to log on to any account (servers, routers, switches, printers) as a system administrator.
   - Sending, accessing, uploading, downloading, or distributing pornographic or sexually explicit materials.
   - Installing, enabling, launching, or creating programs that interfere with the performance of the network, internet, or hardware technology resources.
   - Creating, uploading, or transmitting computer viruses.
   - Attempting to defeat computer or network security.

   Consequences:
   Suspension of chromebook, referral to law enforcement authorities, and possible long term suspension or recommended expulsion from school.

2. Brasher Falls Central School District does not guarantee that its technology resources will be uninterrupted or error-free; nor does it make any warranty as to the results to be obtained from use of the service or the accuracy or quality of the information obtained on or by the network. Access to the network is provided on an "as is" basis without

warranties of any kind. Neither the school district nor any of its agents or employees shall be liable for any direct, indirect, incidental, special, or consequential damages arising out of the use of or inability to use the network or Internet.

3. Users shall be responsible for any costs, fees, charges, or expenses incurred under the person's account in connection with the use of the network or Internet except such costs, fees, charges, and expenses as the school district explicitly agrees to pay.

4. Any security or equipment problems arising from the use of technology resources must be reported to the Technology Department or Main Office.

5. Students will be held responsible for maintaining their individual school chromebook and keeping them in good working order.
    - Chromebook batteries must be charged and ready for school each day.
    - Only labels/stickers approved by BFCSD may be applied to the chromebook.
    - Chromebook bags furnished by the school district must be returned with only normal wear and no alterations to avoid paying a bag replacement fee.
    - Chromebooks that malfunction or are damaged must first be reported to the Technology Department. The school district will be responsible for repairing chromebooks that malfunction. Chromebooks that have been damaged from normal use will be repaired with no cost or minimal cost to the student if there is accidental damage. Students will be entirely responsible for the cost of repairs to chromebooks that are damaged intentionally.
    - Accidental chromebook damage: The district understands that accidental damage can occur to Chromebooks within the normal school day, during transition to home and at home. For this purpose students who experience an initial accident will be spared from any financial penalty. Any student who recorded two or more instances of accidental chromebook damage will be asked to pay up to the retail cost of repair or replacement or the Chromebook or charger as listed in this document at the time of damage.

STUDENT CONTRACT FOR CHROMEBOOK USE
Brasher Falls Central School District

1. I will take good care of my school provided chromebook.
2. I will never leave the school provided chromebook unattended.
3. I will keep food and beverages away from my chromebook as they may cause damage to the computer.
4. I will not disassemble any part of any chromebook/computer or attempt any repairs.
5. I will protect any chromebook/computer by carrying it in the closed position or in an approved case.
6. I will use any chromebook/ computer in ways that are appropriate and educational.
7. I will not write on, carve or put stickers on the District chromebook.
8. I understand that all chromebook/computers and accounts are subject to inspection at any time without notice and remain the property of Brasher Falls Central School District.
9. I understand and agree to follow the criteria described in the District Acceptable Use Policy (#7314).
10. I will follow the policies outlined in the Computer/Chromebook Handbook and the Computer Use Policy while at school, as well as outside the school day.
11. I will be responsible for all damage or loss caused by neglect or abuse.
12. I agree to return the District chromebook to the location I borrowed it from .
13. I will not reveal my own or anyone else's address, phone number, or other personal information.
14. I agree to abide by all copyright and license agreements.
15. I agree that no financial transactions of any kind will be allowed using the school account.
16. I understand that access to the internet will be allowed, as well as the possibility of student work and photos being published on the internet.

Student Name: _____ (Please Print) Grade: _____

Student Signature: _____ Date: _____

Parent Signature: _____ Date: _____

Parent Email: _____