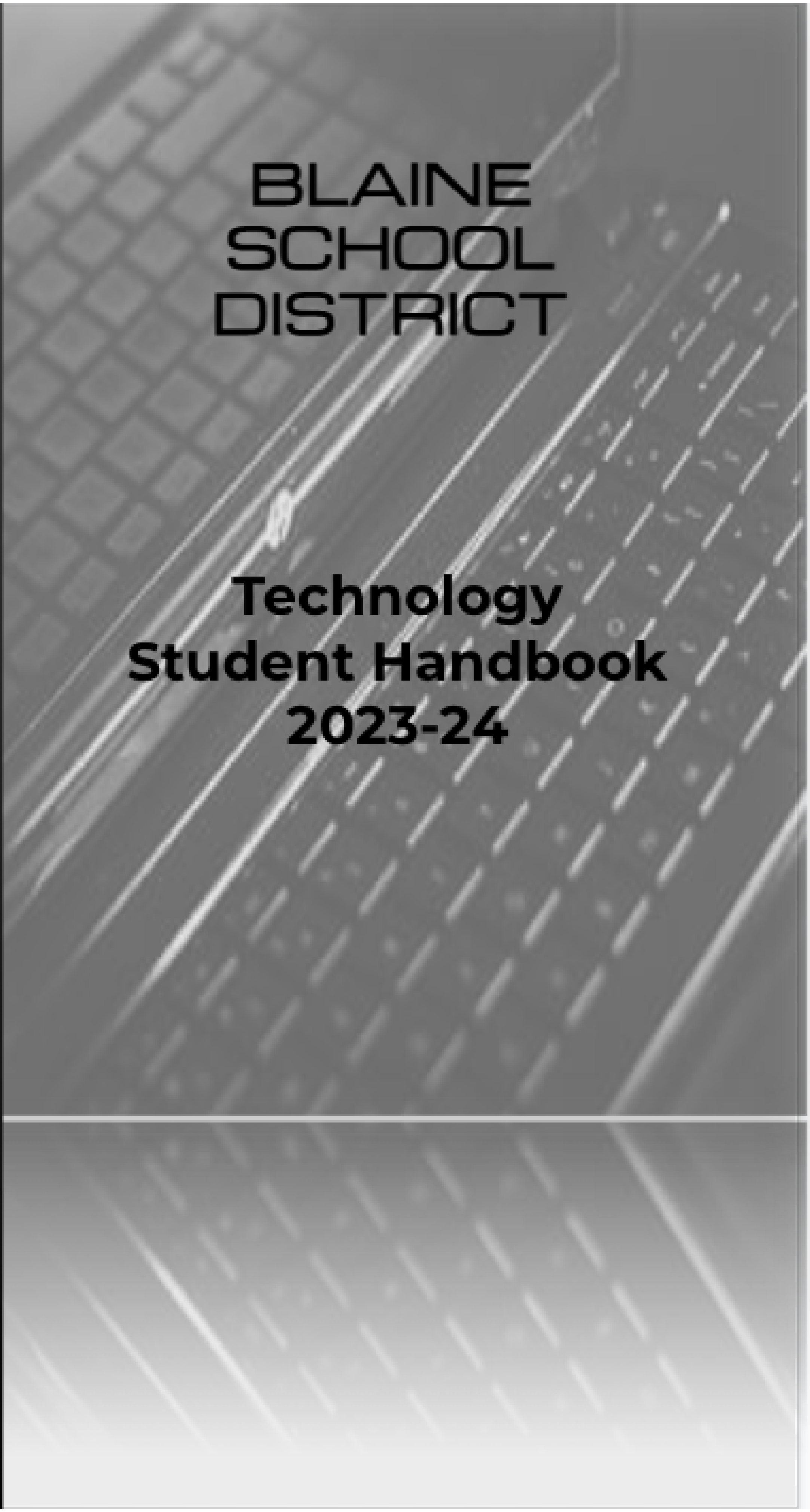

BLAINE SCHOOL DISTRICT

Technology Student Handbook 2023-24

Why District Issued Chromebooks?

- Gives students the opportunity to access real-time information.
- Enables students to create meaningful connections with peers and teachers both on campus and at home.
- District issued chromebooks allow for the design of more individualized programs to meet the needs of students.

Chromebook Monitoring and Filtering

District issued chromebooks allow for internet activity to be filtered through the district server. Because our chromebooks are managed through the district this allows for us to block and monitor content. Internet activity through your home wireless network is not filtered. All activity is logged and monitored when students are logged into their district Google account. Students and Guardians should be aware that **EMAILS ARE NOT CONFIDENTIAL**. Emails are monitored and are considered legal documents.

When Checking Out A District Issued Chromebook Students and Guardians Agree To The Following

STUDENTS

- I agree to follow teachers'/building/district instructions when using technology as stated in my school Student Handbook and the District Technology User Agreement.
- I agree to be polite, considerate, and to use appropriate language.
- I agree to report and/or help prevent any bullying or harm of others.
- I agree to tell an adult if I read, see, or access something inappropriate, or if I witness inappropriate use of technology.
- I agree to follow all filters and security measures.
- I agree to use technology carefully, take care of the equipment, and to conserve district resources.
- I agree not to share my passwords except with my teacher or parent/guardian **(Family Educational Rights and Privacy Act or FERPA)**
- I agree to use only my own files, folders, and account. I will not access another individual's files, folders, or account without their permission.
- I agree to not reveal or post personal information belonging to myself or another person (i.e., passwords, addresses, or telephone numbers).
- I agree to follow copyright laws.

Following federal, state, and local laws, Blaine School District will protect student and employee data. However, I understand that my use of any district technology (computer, network, internet resources, etc.) will be monitored and is neither private nor confidential to district/authorized personnel. I understand that if I violate this agreement, the district's policies and procedures, or my student handbook, I may not be allowed to continue to use technology or I may receive other appropriate consequences.

PARENTS

- I understand that the Blaine school District Electronic Resource Acceptable Use Procedure 2022 explains student requirements for appropriate and responsible use of technology. *(Policy 2022 can be found at the end of this document)
- I understand that the district **may** cover the costs associated with repair/replacement for accidental damage, loss, or theft.
- I understand the district reserves the right to charge the user full cost of repair/replacement when damage or loss is intentional or due to gross negligence as determined by building administrators.
- I understand my student **MUST** return the equipment when requested at the end of the school year or prior to transferring form the Blaine School District.
- I understand that I will be charged for any missing or lost case or power cord.
- I accept responsibility to support my student following the student technology use agreement and the appropriate use of technology resources outside of the school day.

Student Safety

- Students are responsible for what is in their Google Account.
- Students should be careful about information they share from their Google Drive.
- **Once something is posted on social media and online, it is permanent.**
- Respect others: Never post anything rude or offensive.
- If someone makes you feel uncomfortable- **DO NOT RESPOND**, save evidence, tell your parent, guardian, or another trusted adult.
- Keep your passwords strong and secure.
- **DO NOT** leave your device logged in to your Google account and unattended.

Internet Safety Tips for Home

(Please read the Internet Safety Section of the Student User Agreement in the doc

- Keep Vital numbers private
- Establish “house rules”- use your device in a public place in the home.
- Have your student show you what they have learned.

Cyberbullying

What is cyberbullying?

Cyberbullying is bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as cellphones, computers, and tablets as well as communication tools, including social media sites, text messages, chat and websites.

Examples of cyberbullying include mean text messages or emails, rumors sent by email or posted on social media networking sites as well as embarrassing pictures, videos, websites or fake profiles.

Parents/Guardians should discuss cyberbullying with their student(s). The Blaine School District has a zero tolerance policy against cyberbullying and it is considered unacceptable use of district issued technology.

Unacceptable use of the the district's network and electronic resources includes, but is not limited to the following examples which are NOT PERMITTED:

*The following is an excerpt from the K-5 & 6-12 Network User Agreement. All students are required to read and sign this each school year. **(You will find full copies of both agreements at the end of this document)*

"Action constituting harassment, intimidation, or bullying, including cyberbullying, hate mail, defamation, and discriminatory jokes or remarks (This may also include the manufacture, distribution, or possession of inappropriate digital images.)"

Any violation of this agreement or the district's policy and procedure may result in disciplinary action, including but not limited to suspension or revocation of a student's access privilege. Certain violations may constitute a criminal offense, in which case appropriate legal action may be taken.

Storing Chromebooks At School and At ExtraCurricular Activities

- In between classes- carry the chromebook in your district issued case.
- At lunch- keep your case in your possession either by carrying it or hanging it on the back of your chair.
- During PE/Athletics- your chromebook needs to be **LOCKED** in your locker.
- During practice or extracurricular trips- your chromebook needs to be **LOCKED** in your locker. At no time should it travel to games, be left on buses, etc.
- Your chromebook should always be stored and transported in your district issued case. If you have the case in your backpack, be mindful. Screen damage can happen from tossing the backpack.

Cleaning and Care of District Issued Chromebooks

- Use microfiber cloths to clean the screen.
- No Windex or chemicals should be used to clean the chromebook.
- Never spray water directly on the chromebook, spray the cloth and then clean the device.
- Do not apply excessive pressure to the screen.
- Keep the chromebook and power cord clean.
- Keep the device at room temperature at all times. Don't leave it in the car or in the rain.
- Rest the chromebook on a hard surface when in use.
- Make sure the keyboard area is clear before closing the device.
- Do not eat or drink when using or near the device.
- Keep the chromebook in the provided bag when not in use.
- Do not drop or throw the chromebook on the floor, desk or table.
- Open and close the chromebook with care.
- Bundle and store your charger properly.
- Do not pick apart, cut or purposely damage the keyboard, display or casing.
- **Do not place stickers on the chromebook or write on the chromebook.**
- Keep the chromebook and charger away from pets and small children.
- Close your chromebook before moving it.

Preventing Theft

- Keep the device in your possession at all times.
- Do not leave the device unattended.
- Lock the device in your locker if it is not in use.

You could be liable for loss and/or damage. Theft of a laptop will result in legal action. **Failure to return a laptop at the end of the year or at the time of withdrawal from the district will be treated as theft.**

Student Expectations for District Issued Chromebooks

Students are expected to bring their district issued chromebooks and chargers to school/class daily. The device should be fully charged each day. Students should always transport their device in the provided case.

Chromebooks issued to students by the Blaine School District are not personal computers and should be treated with care. The following chart outlines the procedures that will be followed should a student commit any of the following actions**.**

Please review this with your student.

BSD Technology Disciplinary Procedures

	1st Offense	2nd Offense
Use of a device in a way not instructed (games, YouTube, non-academic browsing, etc.)	Parent/Guardian notification, Restricted User account	Referral to administration, Parent/Guardian notification, Loss of device
Intentionally damaging or vandalizing a Chromebook or equipment	Parent/Guardian notification, Invoiced for damages	Referral to administration, Parent/Guardian notification, Loss of device
Damage incurred due to negligence	Parent/Guardian notification, Invoiced for damages	Referral to administration, Parent/Guardian notification, Invoiced for damages, Loss of Device
Use of the device and its capabilities to bully/threaten/cyberbully	Parent/Guardian notification, Restricted User account	Referral to administration, Parent/Guardian notification, Loss of device
Sites, sounds, music, and/or images of a highly sexual nature (pornography)	Parent/Guardian notification, Restricted User account	Referral to administration, Parent/Guardian notification, Loss of device
Violating the academic purpose of technology (private email, shopping, hosting online games,	Parent/Guardian notification, Restricted User account	Referral to administration, Parent/Guardian notification, Loss of device

inappropriate language, misuse of Google apps or Drive)		
Intentionally bypassing network filters or security measures	Parent/Guardian notification, Restricted User account	Referral to administration, Parent/Guardian notification, Loss of device
Manipulation of another student's work or impersonating another user	Parent/Guardian notification, Restricted User account	Referral to administration, Parent/Guardian notification, Loss of device
Habitually bringing an uncharged Chromebook to school or not bringing the Chromebook at all	Parent/Guardian notification	Referral to administration
Device left unattended	Parent/Guardian notification	Referral to administration

The Condition of Your Student’s District Issued Chromebook

Every summer the Technology Department conducts a thorough examination of all district chromebooks. Repairs are made and the devices are prepared for the new school year.If the Technology Department notices any damages to the device or any willful destruction, this is noted in our service log and replacement costs may be assessed. If the device is no longer able to function properly, it will be retired and your student may be charged replacement costs. If the damaged device is in working order, the Technology department will repair and flag the device to be re-issued to the same student at the beginning of the school year.

Please take a moment to visually inspect your student’s device when it is issued. Please note any damage and contact the Technology Department as soon as possible at 360-332-0732. We will confirm whether or not this was previous damage that was noted in our examination of the device.

The Technology Department encourages parents to check their student’s devices regularly to ensure it is in working order and there are no damages. If there are issues or damage to the device contact the Technology Department immediately for repair.

Over the course of the school year, technology checks will be conducted in the classroom well. Any damage or missing components will be reported to the Technology Department and the items will be repaired or replaced. Parents should be aware that replacement costs may be charged.

Chromebook Replacement Costs and Repair Fees-

LCD Screen	$55.00
Keyboard/Palmrest	$43.00
Liquid Damage	life of unit
Dell Chromebook Gen 3	$100.00

Dell Chromebook Gen 4	$150.00
Chromebook Replacement Charger	$30.00
Laptop Case	$15.00
Chromebook Hinge Covers	$5.00
Headphone/USB broken off in jack (no motherboard damage)	$30.00
Sticker Removal	$10.00/sticker
Graffiti Removal	$10.00

The Technology Department will photographically document any and all damages to devices sent for repair. These photos will be linked to the student's Technology Roster Account.

Affordable Connectivity Plan (ACP)

The Blaine School District is no longer issuing hot spots. If your family is in need of the internet at your residence, the Affordable Connectivity Plan (ACP) may be an option for you. For more information visit https://www.affordableconnectivity.gov/

If you have questions or need assistance signing up for ACP, please contact Tricia Johnson at 360-332-0732.

Electronic Resources Acceptable Use Policies and Procedures

*Policy Procedure Form 2022P

K-20 Network Acceptable Use Guidelines/Internet Safety Requirements

These procedures are written to support the Electronic Resources Policy of the board of directors and to promote positive and effective digital citizenship among students and staff. Digital citizenship includes the norms of appropriate, responsible, and healthy behavior related to current technology use. Successful, technologically-fluent digital citizens recognize and value the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world. They cultivate and manage their digital identity and reputation, and are aware of the permanence of their actions in the digital world. Expectations for student and staff behavior online are no different from face-to-face interactions.

Use of Personal Electronic Devices

In accordance with all district policies and procedures, students and staff may use personal electronic devices (e.g. laptops, mobile devices and e-readers) to further the educational and research mission of the district. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day. Absent a specific and articulated need (e.g. assistive technology), students do not have an absolute right to possess or use personal electronic devices at school.

Network

The district network includes wired and wireless devices and peripheral equipment, files and storage, e-mail and Internet content (blogs, websites, collaboration software, social networking sites, wikis, etc.). The district reserves the right to prioritize the use of, and access to, the network. All use of the network must support education and research and be consistent with the mission of the district.

Acceptable network use by district students and staff includes:

A. Creation of files, digital projects, videos, web pages, and podcasts using network resources in support of education and research;
B. Participation in blogs, wikis, bulletin boards, social networking sites and groups, and the creation of content for podcasts, e-mail, and webpages that support education and research;
C. With parental permission, the online publication of original educational material, curriculum-related materials, and student work. Sources outside the classroom or school must be cited appropriately;
D. Staff use of the network for incidental personal use in accordance with all district policies and procedures; or
E. When applicable, connection of personal electronic devices (wired or wireless), when authorized, including portable devices with network capabilities, to the district network after checking with the Technology Director to confirm that the device is equipped with up-to-date virus software, compatible network card, and is configured properly. Connection of any personal electronic device is subject to all procedures in this document and district policy.

Unacceptable network use by district students and staff includes but is not limited to:

A. Personal gain, commercial solicitation, and compensation of any kind;
B. Actions that result in liability or cost incurred by the district;
C. Downloading, installing and use of games, audio files, video files, games, or other applications (including shareware or freeware) without permission or approval from the campus administrator in consultation with the Technology Director);
D. Support for or opposition to ballot measures, candidates, and any other political activity;
E. Hacking, cracking, vandalizing, the introduction of malware, including viruses, worms, Trojan horses, time bombs, and changes to hardware, software, and monitoring tools;
F. Unauthorized access to other district computers, networks, and information systems (including District staff and student Google accounts);
G. Action constituting harassment, intimidation or bullying, including cyberbullying, hate mail, defamation, discriminatory jokes, and remarks. This may also include the manufacture, distribution, or possession of inappropriate digital images;
H. Information posted, sent, or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
I. Accessing, uploading, downloading, storage and distribution of obscene, pornographic, or sexually explicit material
J. Attaching unauthorized devices to the district network. Any such device may be confiscated and additional disciplinary action may be taken; or
K. Any unlawful use of the district network, including but not limited to stalking, blackmail, violation of copyright laws, and fraud.

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

Internet Safety

Personal Information and Inappropriate Content:

A. Students and staff should not reveal personal information, including a home address and phone number on web sites, blogs, podcasts, videos, social networking sites, wikis, e-mail, or as content on any other electronic medium;
B. Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;
C. No student pictures or names can be published on any public class, school or district website unless the appropriate permission has been obtained according to district policy
D. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority; and
E. Students should be aware of the persistence of their digital information, including images and social media activity, which may remain on the Internet indefinitely.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

A. Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites;
B. Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modifications to district browser settings, and any other techniques designed to evade filtering or enable the publication of inappropriate content);
C. E-mail inconsistent with the educational and research mission of the district will be considered SPAM and blocked from entering district e-mail boxes;
D. The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district devices;
E. Staff members who supervise students, control electronic equipment, or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district;
F. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct, and assist effectively;
G. The district may monitor student use of the district network, including when accessed on students' personal electronic devices and devices provided by the district, such as laptops, netbooks, and tablets; and
H. The district will provide a procedure for students and staff members to request access to internet websites blocked by the district's filtering software by contacting the campus administrator who will respond within seven (7) business days. An appeal of the campus administrator's denial can be submitted to the superintendent for reconsideration within seven (7) business days of the denial. The requirements of the Children's Internet Protection Act (CIPA) will be considered in evaluation of the request.

Internet Safety Instruction

All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response:

A. Age appropriate materials will be made available for use across grade levels; and
B. Training on online safety issues and materials implementation will be made available for administration, staff, and families.

Copyright

Downloading, copying, duplicating, and distributing software, music, sound files, movies, images, or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

Ownership of Work

All work completed by employees as part of their employment will be considered property of the district. The District will own any and all rights to such work including any and all derivative works, unless there is a written agreement to the contrary.

All work completed by students as part of the regular instructional program is owned by the student as soon as it is created, unless such work is created while the student is acting as an employee of the school system or unless such work has been paid for under a written agreement with the school system. If under an agreement with the district, the work will be considered the property of the district. Staff members must obtain a student's permission prior to distributing his/her work to parties outside the school.

Network Security and Privacy

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized district purposes. Students and staff are responsible for all activity on their account and must not share their account password.

The following procedures are designed to safeguard network user accounts:

A. Change passwords according to district policy;
B. Do not use another user's account;
C. Do not insert passwords into e-mail or other communications;
D. If you write down your user account password, keep it in a secure location;
E. Do not store passwords in a file without encryption;
F. Do not use the "remember password" feature of Internet browsers; and
G. Lock the screen or log off if leaving the computer.

Student Data is Confidential

District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

No Expectation of Privacy

The district provides the network system, e-mail, and Internet access as a tool for education and research in support of the district's mission. The district reserves the right to monitor, inspect, copy, review, and store, without prior notice, information about the content and usage of:

A. The district network, including when accessed on students' personal electronic devices and on devices provided by the district, such as laptops, netbooks, and tablets;
B. User files and disk space utilization;

C. User applications and bandwidth utilization;
D. User document files, folders and electronic communications;
E. E-mail;
F. Internet access; and
G. Any and all information transmitted or received in connection with network and e-mail use.

No student or staff user should have any expectation of privacy when using the district's network. The district reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington.

Educational Applications and Programs

District staff may request students to download or sign up for applications or programs on the students' personal electronic devices. Such applications and programs are designed to help facilitate lectures, student assessment, communication, and teacher-student feedback, among other things.

Prior to requesting students to download or sign up for educational applications or programs, staff will review "terms of use," "terms of service," and/or "privacy policy" of each application or program to ensure that it will not compromise students' personally identifiable information, safety, and privacy. Staff will also provide notice in writing of potential use of any educational application or program to the campus administrator, including the anticipated purpose of such application or program. Specific expectations of use will be reviewed with students.

Staff should also, as appropriate, provide notice to students' parents/guardians that the staff person has requested that students download or sign up for an application or program, including a brief statement on the purpose of application or program.

Archive and Backup

Backup is made of all district e-mail correspondence for purposes of public disclosure and disaster recovery. Barring technical issues, staff and student files are backed up regularly. Refer to the district retention policy for specific records retention requirements.

Disciplinary Action

All users of the district's electronic resources are required to comply with the district's policy and procedures (and agree to abide by the provisions set forth in the district's user agreement). Violation of any of the conditions of use explained in the district's user agreement, Electronic Resources policy, or in these procedures may be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges.

Accessibility of Electronic Resources

Federal law prohibits people, on the basis of disability (such as seeing and hearing impairments), from being excluded from participation in, being denied the benefits of, or otherwise being subjected to discrimination by the district. To ensure that individuals with disabilities have equal access to district programs, activities, and services, the content and functionality of websites associated with the district should be accessible. Such websites may include, but are not limited to, the district's homepage, teacher websites, district-operated social media pages, and online class lectures.

District staff with authority to create or modify website content or functionality associated with the district will take reasonable measures to ensure that such content or functionality is accessible to individuals with disabilities. Any such staff member with questions about how to comply with this requirement should consult with the District's Public Relations Specialist**.**

Blaine School District -Policy 2022

Electronic Resources and Internet Safety-

**Student User Agreement K-5th Grade Students

The following acceptable use guidelines include excerpts from Blaine School District Policy 2022 and its accompanying Procedure 2022P. The complete policy and procedure, as well as this agreement, are accessible from the district's website. These guidelines are written to promote positive and effective digital citizenship among students. Digital citizenship includes the norms of appropriate, responsible, and healthy behavior related to current technology use. Successful, technologically-fluent digital citizens recognize and value the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world. They cultivate and manage their digital identity and reputation, and are aware of the permanence of their actions in the digital world. Expectations for student behavior online are no different from face-to-face interactions.

Network and Account Use: The district network includes wired and wireless devices and peripheral equipment, files and storage, e-mail and Internet content, including Google for Education accounts and content. Use of the network is a privilege, not a right, and inappropriate use may result in suspension or revocation of those privileges. No user should have any expectation of privacy when using the district's network. As a component of district Internet safety measures, all district-owned electronic resources capable of accessing the Internet must use filtering software to prevent access to obscene, racist, hateful or violent material. However, given the ever-changing nature of the Internet, the district cannot guarantee that a student will never be able to access objectionable material. The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data or unauthorized financial obligations resulting from network use or access.

Acceptable use of the district's network and electronic resources includes any use in support of education and educational research as detailed in the district's policy and procedure.

Unacceptable use of the district's network and electronic resources includes, but is not limited to, the following examples which are **NOT PERMITTED**:

1. Displaying or distributing pictures or messages deemed inappropriate by administrators/staff

2. Using obscene language or material

3. Damaging computers, computer system, or computer networks

4. Any unlawful use of the district network, including but not limited to stalking, blackmail, fraud, and violation of copyright laws (i.e. downloading, copying, duplicating, and distributing software, music, sound files, movies, images, or other copyrighted materials without the specific written permission of the copyright owner)

5. Using other users' passwords or trespassing on other users' systems, folders, work, or files

6. Excessive use of limited resources (beyond time authorized by administrators/staff)

7. Utilizing the network for commercial, personal, or political purposes

8. Personal email or free “web surfing” during school hours

9. Modifying software on district equipment or installing games, files, or applications without permission

10. Accessing any computer not explicitly authorized for use

11. Action constituting harassment, intimidation or bullying, including cyberbullying, hate mail, defamation, and discriminatory jokes or remarks (This may also include the manufacture, distribution, or possession of inappropriate digital images.)

12. Bypassing district filters and/or accessing filtered sites or material (e.g. Facebook, Instagram, etc.)

Internet Safety: Students should observe the following procedures in order to ensure safe and secure online use.

1. **Do not** reveal personal information (i.e. complete name, address, phone number, or identifiable photos) on web sites, blogs, podcasts, videos, social networking sites, wikis, e-mail, or as content on any other electronic medium.

2. **Do not** reveal personal information about another individual on any electronic medium without first obtaining permission.

3. **Do not** agree to meet anyone in person whom you have been in contact with online without parent permission.

4. **Tell** your teacher or other school employee if you encounter dangerous or inappropriate information or if you receive any message that is inappropriate or makes you feel uncomfortable.

5. **Be aware** of the persistence of your digital information, including images and social media activity, which may remain on the Internet indefinitely.

Use of Personal Electronic Devices: Students may use personal electronic devices to further the educational and research mission of the district. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day. Absent a specific and articulated need (e.g. assistive technology), students do not have an absolute right to possess or use personal electronic devices at school.

Communication: Blaine School District will provide access to applications and programs for communication between students, staff, and parents (e.g. Google for Education, Remind, etc.) Students are expected to use these resources for school-related electronic communication with teachers and staff.

PARENT OR GUARDIAN – signature required. Form can be found and signed electronically in Skyward in Family Access.

As a parent or guardian of the student named below, I have read the Electronic Resources User Agreement. I agree and understand:

Access to the district’s network and electronic resources is designed for educational purposes only.

It is impossible for Blaine School District to completely restrict access to offensive, inappropriate, or other controversial information and materials available through the Internet or other sources from the network.

I will not hold the school district responsible for information and materials obtained by this student on the network.

I will support my student’s responsible use of the district’s network as described in this agreement.

Any violation of this agreement, or the district’s policy and procedure, may result in disciplinary action, including but not limited to suspension or revocation of my student’s access privilege. I further understand that certain violations may constitute a criminal offense, in which case appropriate legal action may be taken.

I accept full responsibility for supervision if and when my student uses their provided user account to access the network outside of the school setting.

This agreement will be kept on file at the school.

Blaine School District -Policy 2022

Electronic Resources and Internet Safety-

**Student User Agreement 6th-12th Grade Students

The following acceptable use guidelines include excerpts from Blaine School District Policy 2022 and its accompanying Procedure 2022P. The complete policy and procedure, as well as this agreement, are accessible from the district’s website. These guidelines are written to promote positive and effective digital citizenship among students. Digital citizenship includes the norms of appropriate, responsible, and healthy behavior related to current technology use. Successful, technologically-fluent digital citizens recognize and value the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world. They cultivate and manage their digital identity and reputation, and are aware of the permanence of their actions in the digital world. Expectations for student behavior online are no different from face-to-face interactions.

Network and Account Use: The district network includes wired and wireless devices and peripheral equipment, files and storage, e-mail and Internet content, including Google for Education accounts and content. Use of the network is a privilege, not a right, and inappropriate use may result in suspension or revocation of those privileges. No user should have any expectation of privacy when using the district’s network. As a component of district Internet safety measures, all district-owned electronic resources capable of accessing the Internet must use filtering software to prevent access to obscene, racist, hateful or violent material. However, given the ever-changing nature of the Internet, the district cannot guarantee that a student will never be able to access objectionable material. The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data or unauthorized financial obligations resulting from network use or access.

Acceptable use of the district’s network and electronic resources includes any use in support of education and educational research as detailed in the district’s policy and procedure.

Unacceptable use of the district's network and electronic resources includes, but is not limited to, the following examples which are **NOT PERMITTED:**

1. Displaying or distributing pictures or messages deemed inappropriate by administrators/staff (e.g. sexually explicit, pornographic, obscene, lewd, or in other ways inappropriate).

2. Using obscene language or material.

3. Damaging computers, computer systems, or computer networks.

4. Any unlawful use of the district network, including but not limited to stalking, blackmail, fraud, and violation of copyright laws (i.e. downloading, copying, duplicating, and distributing software, music, sound files, movies, images, or other copyrighted materials without the specific written permission of the copyright owner).

5. Using other users' passwords or trespassing on other users' systems, folders, work, or files.

6. Excessive use of limited resources (beyond time authorized by administrators/staff).

7. Utilizing the network for commercial, personal, or political purposes.

8. Personal email or free "web surfing" during school hours.

9. Modifying software on district equipment or installing games, files, or applications without permission.

10. Accessing any computer not explicitly authorized for use.

11. Action constituting harassment, intimidation or bullying, including cyberbullying, hate mail, defamation, and discriminatory jokes or remarks (This may also include the manufacture, distribution, or possession of inappropriate digital images.).

12. Bypassing district filters and/or accessing filtered sites or material (e.g. Facebook, Instagram, etc.).

Internet Safety: Students should observe the following procedures in order to ensure safe and secure online use.

1. **Do not** reveal personal information (i.e. complete name, address, phone number, or identifiable photos) on web sites, blogs, podcasts, videos, social networking sites, wikis, e-mail, or as content on any other electronic medium.

2. **Do not** reveal personal information about another individual on any electronic medium without first obtaining permission.

3. **Do not** agree to meet anyone in person whom you have been in contact with online without parent permission.

4. **Tell** your teacher or other school employee if you encounter dangerous or inappropriate information or if you receive any message that is inappropriate or makes you feel uncomfortable.

5. **Be aware** of the persistence of your digital information, including images and social media activity, which may remain on the Internet indefinitely.

Use of Personal Electronic Devices: Students may use personal electronic devices to further the educational and research mission of the district. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day. Absent a specific and articulated need (e.g. assistive technology), students do not have an absolute right to possess or use personal electronic devices at school.

Communication: Blaine School District will provide access to applications and programs for communication between students, staff, and parents (e.g. Google for Education, Remind, etc.) Students are expected to use these resources for school-related electronic communication with teachers and staff.

STUDENT – required to sign. Form can be found and signed electronically in Skyward in Family Access.

I understand and will abide by this Electronic Resources User Agreement, as well as the district's policy and procedure, and I agree to use the network responsibly. I further understand that any violation of the regulations contained therein may result in disciplinary action and may constitute a criminal offense. Should I commit any violation, my access privileges may be suspended or revoked and school disciplinary action or appropriate legal action may be taken.

PARENT OR GUARDIAN – signature required if student is under 18 or if adult student is living at home or with guardian Form can be found and signed electronically in Skyward in Family Access.

As a parent or guardian of this student, I have read the Electronic Resources User Agreement. I agree and understand: Access to the district's network and electronic resources is designed for educational purposes only. It is impossible for Blaine School District to completely restrict access to offensive, inappropriate, or other controversial information and materials available through the Internet or other sources from the network. I will not hold the school district responsible for information and materials obtained by this student on the network. I accept full responsibility for supervision if and when my student uses their provided user account to access the network outside of the school setting. This agreement will be kept on file at the school. I hereby give permission for this student to have Internet access, and I certify that the information contained on this form is correct.

Technical Support

Please do not attempt to repair your chromebook. If your student has a chromebook that needs repair, they can drop it off in the following locations.

Primary- Primary School Office

Elementary- Elementary School Office

Middle School- Middle School Office

High School- Main Office

HomeConnections- Call 360-332-0732

Pt. Roberts Primary- Call 360-332-0732

If a student has lost or damaged their power charger, please contact Tech Support for a replacement. **PLEASE DO NOT PURCHASE AFTER MARKET CHARGERS Or Return with an After market charger.**

Items needing repair will be collected from the above locations and returned to the student. Most repairs are returned on the same day. If repairs will take longer the Technology Department will notify the student or their teacher.

Technical support is available Monday- Friday 8:00 am to 3:00 pm. If you are having technical concerns please contact Tech Support via techhelp@blainesd.org.

Chromebook Troubleshooting Tips

NOT CHARGING/NOT TURNING ON

If your Chromebook isn't charging, or not turning on, please check the following items:

1. Check all power connections. Remove any power strips and surge protectors then connect the AC power adapter directly to the ac power outlet.
2. Inspect the AC power adapter. Check for any physical damage, and make sure that the power cable is firmly attached to the adapter brick and to the Chromebook.
3. **After verifying these items have been checked. Proceed with a Hardware Reset. Follow the steps below to perform a Hardware Reset.**
4. Plug in your Chromebook

5. Press and hold the **Refresh** ↻ key and press the **Power button** once**.**

6. When your Chromebook charge light turns on, release the Refresh ↻ key

7. It takes up to ten seconds for the device to boot-up. If nothing happens after ten seconds, press the **power button** to turn on Chromebook.

If your Chromebook still doesn't turn on or charge you may have faulty hardware and it will need to be diagnosed by a technician at the IT office. Please take your device and charger to the office. Office staff will contact the IT Department to come and collect your computer for repair.

TOUCHPAD / CAMERA / KEYBOARD / ETC. NOT WORKING

If a specific piece of hardware on your Chromebook stops working. Examples include: touchpad, keyboard, USB port(s), headphone jack, camera.

1. Turn off your Chromebook, then turn it back on
2. Perform a Hardware Reset
3. Please refer to the problem above for instructions on how to do this.

IF YOUR NON-FUNCTIONING HARDWARE STILL ISN'T WORKING, YOUR DEVICE WILL NEED TO BE DIAGNOSED BY A TECHNICIAN IN THE BSD IT DEPARTMENT. PLEASE TAKE YOUR DEVICE TO YOUR BUILDING OFFICE. BE SURE THE COMPUTER IS IN ITS PROTECTIVE CASE, INCLUDING THE CHARGER AND A NOTE WITH THE ISSUE YOU ARE HAVING. THE IT DEPARTMENT WILL COLLECT AND REPAIR THE DEVICE AND RETURN IT TO THE BUILDING OFFICE USUALLY WITHIN A FEW HOURS OF RECEIVING IT.

RUNNING SLOW OR LAGGING

If your Chromebook is slow, check for the newest version of chrome operating system

1. On your computer, open Chrome.
2. At the top right, click More .
3. Click **Help** and then **About Google Chrome**.
4. Click **Update Google Chrome**.
5. **Important**: If you can't find this button, you're on the latest version.
6. Click **Relaunch**.