Greenfield-Central Community School Corporation
Responsible Use Policy for Technology Resources

Introduction:
Greenfield-Central Community School Corporation (G-C CSC) recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop progressive technology and communication skills.

G-C CSC is committed to providing educational opportunities for all students and maintains compliance with the Individuals with Disabilities Education Act 2004 (20 U.S.C. 1400 et seq.).

To that end, we provide the privilege of access to technologies for student and staff use.

This Responsible Use Policy outlines the guidelines and behaviors that all users are expected to follow when using school technologies or when using personally-owned devices on the school campus, as every member of the G-C CSC community is responsible for their actions and activities involving the school district's computers, electronic devices, network and Internet services, regardless of how these are accessed, and for their computer files, passwords and accounts. These guidelines and behaviors provide general guidance concerning the use of school computers and other electronic devices and provide examples of prohibited uses.

The rules do not attempt to describe every possible prohibited activity. Users must comply with all Board policies, the student handbook, and school rules and expectations concerning conduct and communications when using school computers or school-issued electronic resources, whether on or off school property. Students also must comply with all specific instructions from school staff. To that end, guidelines and behaviors within this RUP include:

- The G-C CSC network is intended for educational purposes.
- All activity over the network or using district technologies may be monitored, documented and retained.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA) and confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources can result in disciplinary action.
- Using an internet filter and other technologies, G-C Schools makes a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the district network or other technologies are expected to alert school corporation staff immediately of any concerns for safety or security.

Students, parents and school staff who have questions about whether a particular activity is prohibited are encouraged to contact a building administrator.

Technologies Covered

This Responsible Use Policy applies to both school-owned technology equipment utilizing the G-C CSC network, the G-C CSC internet connection, and/or private networks/internet connections accessed from school-owned devices at any time. This Responsible Use Policy also applies to privately-owned devices accessing the G-C CSC network, the G-C CSC internet connection, and/or private networks/internet connections while on school property. As relevant new technologies emerge, G-C CSC will seek to provide access to them. The policies outlined in this document cover *all* available technologies now and in the future, not just those specifically listed or currently available.

Usage Policies

All technologies provided by the district are intended for education purposes. Staff members on leave may be asked to leave computer equipment for their substitute. All users are expected to use good judgment and to follow the specifics as well as the spirit of this document. Users should be safe, appropriate, careful and kind; not try to get around technological protection measures; use good common sense; and ask if they don't know.

Web Access

G-C CSC provides its users the privilege of access to the internet, including web sites, resources, content, and online tools.   Access to the internet will be restricted as required to comply with CIPA regulations and school policies. Web browsing may be monitored, and web activity records may be retained indefinitely.

Users are expected to respect the web filter as a safety precaution, and shall not attempt to circumvent the web filter when browsing the internet. The determination of whether material is appropriate or inappropriate is based solely on the content of the material and the intended use of the material, not on whether a website has been blocked or not.   If a user believes a site is unnecessarily blocked, the user should submit a request for website review through the G-C CSC Technology Help Desk Service Ticket or restricted access screen.

Email and other Education Accounts including Social/Web 2.0/Collaborative Content

Users, including Students, may be issued a school email address and other education accounts to improve staff/student communication and collaboration on school projects. All accounts shall be used only for educational purposes that directly relates to a school project or assignment. If users are provided with accounts, the account(s) should be used with care. Users should be careful not to share personally identifying information online; should not attempt to open files or follow links from unknown or untrusted origins; should use appropriate language; and should only communicate with other people as allowed by the district policy or the teacher. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived. In other education accounts, posts, chats, sharing, and messaging may be monitored. Please refer to the **Greenfield-Central Community School Corporation Social Media Policy** for additional information on social communication.

Social Media Policy

G-C CSC will filter public facing social media for students on any of our networks and/or corporation-issued mobile devices. Students should not attempt to bypass these filter settings. There are social media guidelines in place for staff and students, should users take part in internal educational activities that simulate the collaborative nature of social media (i.e blogs, back-channel chats, newsfeeds, etc). These guidelines are suggested for use of social media outside corporation use as well, to help protect our staff and students while online.

Personally Owned Devices Policy
All users are bound to policies stated in the student handbook regarding electronic devices in their school.

In some cases, a separate network may be provided for personally owned devices. Please remember, this Responsible Use Policy applies to privately owned devices accessing the G-C CSC network, the G-C CSC internet connection, and private networks/internet connections while on school property. Please refer to each building's **BYOD Policy** (or the G-CHS Cell Phone Policy) for additional details.

Mobile Devices Policy
G-C CSC may provide users with mobile computers or other devices to promote learning outside of the classroom. Users should abide by the same Responsible Use Policies when using school devices off the school network as on the school network.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to users' care. Users should immediately report any loss, damage, or malfunction to IT staff. Users may be financially accountable for any damage resulting from negligence or misuse. See the additional rules for Laptops, iPads, or other Electronic Devices Issued to Students or Staff as listed in the Greenfield-Central Community School Corporation Digital Learning Technology Handbook for 1:1 MacBook Air Devices. Use of school-issued mobile devices off the school network may still be monitored.

Security
Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. Users should never share personal information.

If users believe a computer or mobile device they are using might be infected with a virus, they should alert IT. Users should not attempt to remove the virus themselves or download any programs to help remove the virus.

Any user who identifies a security problem must notify his/her teacher or building administrator immediately. The user shall not demonstrate the problem to others or access unauthorized material. Staff shall immediately report any potential security breaches to the G-C CSC Technology Department.

Downloads
Users should not download or attempt to download or run programs over the school network or onto school resources without express permission from IT staff.

Users may be able to download other file types, such as images of videos. For the security of the network users should download such files only from reputable sites, and only for education purposes.

Netiquette
Users should always use the internet, network resources, and online sites in a courteous and respectful manner.

Users should recognize that among the valuable content online there is also unverified, incorrect, or inappropriate content. Users should only use trusted sources when conducting research via the internet.

Users should remember not to post anything online that they wouldn't want students, parents, teachers, or future colleges or employers to see. Once something is online, it cannot be completely retracted and can sometimes be shared and spread in ways the user never intended.

Cyberbullying
Cyberbullying will not be tolerated. Harassing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Users should not be mean or send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that online activities may be monitored and retained.

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.

Examples of Responsible Use
 I will:

- Use school technologies for school-related activities.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat school resources carefully and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits.
- Cite sources when using online sites and resources for research.
- Recognize that use of school technologies is a privilege and treat it as such.
- Be cautious to protect the safety of others and myself. For example, staff may post student pictures on district/school/classroom "public" websites as long as information included is public directory information, including a student's first and last name, grade level, school building, honors or awards, and participation in officially recognized activities or athletics. However, students must obtain permission from a G-C CSC staff member to publish a photograph or video of any school-related activity. It is best practice and common courtesy to ask permission before recording an individual or groups. G-C CSC retains all rights concerning any recording and/or publishing of any student's or staff member's work(s) or image(s).
- Help to protect the security of school resources. For example, students' grades, test results, or identifying pictures may be stored only on district-approved secure sites that require a username and password for authorized individuals to access.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Examples of Irresponsible and Prohibited Use
I will **NOT** :

● Use school technologies in a way that could be personally or physically harmful.
● Distribute personally identifying information, about others or myself, including a home address and phone number.
● Use school technologies for non-school related purposes, unless the incidental personal use (use by an individual for occasional personal communications) does not interfere with the user's responsibilities and performance, does not interfere with the system operations or other system users, or does not violate this policy with its accompanying rules or other Board policy/procedure/rules.
● Attempt to find inappropriate images or content.
● Engage in cyberbullying, harassment, or disrespectful conduct toward others.
● Try to find ways to circumvent the school's safety measures and filtering tools.
● Use school technologies to send spam or chain mail.
● Plagiarize content I find online. Plagiarizing content occurs when users use content as their own, without citing the original creator, including words or images, from the internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Information obtained via the internet should be appropriately cited, giving credit to the original author.
● Use cameras in any type of electronic device in locker rooms or restrooms.
● Agree to meet in person someone I meet online.
● Use language online that would be inappropriate in the classroom.
● Use school technologies for illegal activities or to pursue information on such activities.
● Attempt to hack or access sites, servers, or content that isn't intended for my use.
● Waste system resources, such as but not limited to excessive printing through the tech cadets, online gaming, video/audio streaming not directly related to educational projects as determined by the supervising instructor or building principal.
● Attach unauthorized equipment, including personal mobile devices, to the district's secured network without permission from the G-C CSC Technology Department.

This is **not** intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Disclaimer of Limitation of Liability – G-C CSC, its employees and agents, make no warranties of any kind, neither expressed nor implied, concerning the network, Internet access, and electronic resources it is providing. Furthermore, G-C CSC is not responsible for:

1. The accuracy, nature, quality, or privacy of information stored on local servers or devices or information gathered through Internet access.
2. Any damages suffered by a user (whether the cause is accidental or not) including but not limited to, loss of data, delays or interruptions in service, and the infection of viruses or other malware on personal computers or other devices.
3. Unauthorized financial obligations resulting from the use of G-C CSC electronic resources.

Terms of Use
G-C CSC reserves the right to deny, revoke or suspend specific user privileges and/or take other disciplinary action, such as suspensions or expulsion from school, for violations of this policy. Additionally, all handbook regulations apply to the use of the G-C CSC network, Internet, and electronic resources.