GREEN Charter Schools Acceptable Use Policy

Please note that Policy outlined below is the School's Acceptable Use Policy in its entirety and applies to all GREEN staff, students, and families.

Overview

At GREEN Charter Schools, we recognize that technology is an essential component of the educational process. These guidelines are provided for students and staff at GREEN Charter Schools to inform them of their responsibilities while using school-owned electronic devices or personal electronic devices while on GREEN property. All users shall make efficient, ethical, and legal use of the network resources and devices. Any violations of these guidelines may subject the user to appropriate disciplinary action, denial of access to the Internet, and loss of privileges to use a GREEN-owned device.

Access to the GREEN network and school electronic devices provides connections to other computer systems around the world, therefore, users (including the parents/legal guardians of students who are users) should understand that neither GREEN nor any members of its staff control the content of the information available on these systems. The School will make every effort to monitor and restrict ready access to known objectionable sites. However, the School does not condone the use of controversial or offensive materials and shall not be held responsible for such use. GREEN is committed to protecting our students, employees, partners, and the School from illegal or damaging actions taken by individuals, either knowingly or unknowingly.

Internet and Intranet systems, including computer equipment, Chromebooks, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of GREEN Charter Schools. These systems are to be used by our students and staff during normal hours of operation for educational purposes and to serve the School's interests. As such, there is no expectation of privacy, and all users should understand that technology resources at GREEN are a privilege and should not be abused under any circumstances.

Purpose

This agreement outlines the responsible use of computer equipment at GREEN. These rules comply with the Children's Internet Protection Act (CIPA) enacted by Congress in 2000 to address concerns about children's access to obscene or

harmful content over the Internet and to protect students. Inappropriate use may also expose GREEN Charter Schools to risks such as virus/malware and brute force attacks, as well as other forms of ransomware which could compromise our network systems and services and create legal issues.

Scope

This agreement applies to the use of information, electronic and computing devices, and network resources used to conduct GREEN business or interact with internal networks, the Internet, and business systems, whether owned or leased by GREEN, the student, the parent/legal guardian, the employee, or a third party. All students, staff (including permanent, part-time, and temporary), contractors, consultants, and volunteers of GREEN Charter Schools are responsible for exercising good judgment regarding the appropriate use of information, electronic devices, and network resources in accordance with School policy and in adherence to federal and state law. This policy applies to all equipment that is owned or leased by GREEN Charter Schools.

Guidelines

Responsible Use

Under no circumstances is a student or employee of GREEN authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing GREEN networks or equipment. GREEN reserves the right to take immediate action regarding activities that (1) create security and/or safety issues for GREEN, its students, employees, schools, network, or computer resources; or (2) expend GREEN resources on content which GREEN determines to lack legitimate educational purpose; or (3) expose students or staff to content the School deems inappropriate.

The lists below are not exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited:

1. Violating the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not licensed for use by GREEN Charter Schools.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which GREEN or the end user does not have an active license.
3. Accessing inappropriate material on School-provided networks which may include tasteless material, pornographic imagery, sexually explicit or suggestive material, illegal movie websites, or the like.
4. Staff may not place any stickers, decals, or additional markings on GREEN-issued devices.

5. Using "VPNS," "Proxies," or any other form of software or website intended to mask a device's identity or circumvent security and/or content controls at GREEN. Installing such software on a personal device connected to the Students, Staff, Provisioning, and/or Guest networks is strictly prohibited.

6. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

7. Revealing an account password to others or allowing the use of your account by others. This includes family and other household members when work is being completed at home.

8. Using a GREEN computing asset to actively engage in transmitting material that is in violation of sexual harassment policies and laws.

9. Creating security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee/student is not an intended recipient or logging into a server or account that the student or employee is not expressly authorized and/or directed to access. For this section's purposes, "disruption" includes network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification and approval is received from GREEN's IT Manager or their designee.

11. Utilizing any form of network monitoring.

12. Circumventing user authentication or security of any host, network, or account.

13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet or Intranet.

Email Communication & Privacy

When using school resources to access and use the Internet, users represent the School. All chats and emails are logged and monitored, and there should be no expectation of privacy. **All web traffic, email messages, and chat messages are logged and audited periodically.**

GREEN 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. GREEN will fully cooperate with local, state, or federal officials in any lawful investigation concerning or relating to any illegal activities conducted through GREEN Systems. By accessing any data network at GREEN with a personal device, the end-user agrees to reveal the device's IP address, device name, and any content upon request to the GREEN Administration, including to the IT Manager.

The following activities are strictly prohibited:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising or solicitation material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Use of profanity, or any other explicit/suggestive language/imagery.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any type.

Cell Phones and Personal Electronic Devices

- **Students are prohibited from using cell phones/personal electronic devices in any capacity or for any purpose during designated school hours without prior teacher or administration approval. This includes, but is not limited to, during clubs, tutoring, and after-school care.** Failure to follow cell phone

procedures may result in confiscation of the cell phone. Parents may retrieve the phone from the administrator who confiscated it or from the main office at the end of the day. This same policy applies to smart watches. GREEN will not be held responsible for the theft, loss, or damage to cell phones or other electronic devices brought onto its property.

- Staff and students are not permitted to connect their cell phones or personal devices to any GREEN data network. This includes digital picture frames and other personal electronic devices.
- The responsibility to keep electronic devices secure rests with the individual owner. GREEN, its staff, volunteers, or employees, will not be liable for any device which is stolen or damaged on campus.
- If a device is stolen or damaged, it must be reported to the school office immediately.
- It is recommended that appropriate skins (decals) and other custom touches be used to physically identify your **Personal Device *(Not School Owned Devices)*.** Additionally, protective cases for technology are strongly encouraged.
- These electronic devices have educational and monetary value. Students are prohibited from trading or selling these items to other students on school property, including on school buses and during field trips.
- Each student is responsible for their own device, including set-up, maintenance, charging, and security.

GREEN Chromebook Guidelines

1. The use of GREEN-issued Chromebooks and the GREEN network must support education.

2. Students and families must follow all guidelines set forth in this document and by school staff.

3. All rules and guidelines are in effect before, during, and after school hours for all school Chromebooks whether on or off campus.

4. Students are required to keep their Chromebooks in good condition. If the Chromebook breaks or is damaged, the parent/legal guardian student will be held responsible for the cost of repair/replacement.

5. Students are expected to report any damage to their device as soon as possible. This means within 24 hours of the damage occurring if off-campus and immediately if on-campus.

6. Students who identify or are aware of a potential security issue on their Chromebook are expected to convey the details to their teacher without discussing it with other students.

7. Students are expected to notify a staff member immediately if they come across information, images, or messages that are inappropriate, dangerous, threatening, indicate harm to themselves or others, or make them feel uncomfortable.

8. Students may only log in under their assigned GREEN username. Students may not share their passwords with other students at any time. While a parent/legal guardian may be aware of the password for supervision purposes, the student is responsible for all actions associated with the Chromebook and its use. No other family member should have access to the password.

9. Students may not loan Chromebook components to any other person (including family members) for any reason; Students who do so will be held financially responsible for any damage or loss of components.
10. Students are responsible for charging the Chromebook fully at the end of each day. The student is responsible for placing the Chromebook in a safe location and ensuring that the power cord is connected to the Chromebook each evening.
11. Chromebooks are to be stored on a desk or table. Books and/or binders and other items should never be placed on top of a Chromebook. Chromebooks should never be placed on the floor when at school or at home.
12. Chromebooks should never be out or open if a student is consuming food or drink.
13. Chromebooks should not be left in vehicles.
14. Chromebooks should be completely shut down before traveling.
15. Students are not permitted to place any stickers, decals, or additional markings on GREEN-issued Chromebooks.
16. Students are not permitted to use the Webcam on the Chromebook for "personal use." Webcams should only be used for educational purposes. Parents/legal guardians are responsible for supervising students' use of webcams.
17. Students should not use their Chromebooks to watch streaming content such as movies for personal use or to interact with others on any form of social media.

Chromebook Damage Policy

Accidental Damage vs. Negligence

Accidents happen. There is a difference, however, between an accident and negligence, with the latter potentially leading to disciplinary action and/or financial reimbursement to the school. Damages to Chromebooks caused by a student's failure to follow the guidelines set forth in this manual will be deemed negligence. If the Chromebook is deemed to be intentionally or negligently damaged by the student, the student/parent will be held financially responsible for the cost of repair/replacement, and the student may also be subject to disciplinary action if appropriate. Parents/legal guardians will be notified of the repair cost and invoiced. Costs can include the Chromebook, charger, fees/taxes, case/cover, and associated licenses.

Enforcement of Acceptable Use Agreement

Student Non-Compliance with the Acceptable Use Agreement

The guidelines set forth in this document outline the general behaviors that are acceptable and non-acceptable while utilizing GREEN-owned equipment and wireless networks. We also understand that there are times a student may unintentionally violate these guidelines. We will thoroughly investigate each incident and consider both intent and impact as we determine consequences.

Consequences for Non-Compliance

The utilization of electronic devices at GREEN is a privilege. The following disciplinary measures may be taken at the discretion of the GREEN Administration and/or the IT Manager if a student is found to be in violation of this Acceptable Use Agreement on either a personal device or a school-owned device:

→ The student's personal device and GREEN-owned device access may be suspended for a period ranging from one (1) day through the rest of the school year.

→ Students may also face disciplinary action consistent with the GREEN Student Code of Conduct, including In-School Suspension, Out-of-School Suspension, and Expulsion.

Parent/Legal Guardian Responsibilities

GREEN Charter Schools makes every effort to equip parents/legal guardians with the necessary tools and information to ensure the safe and responsible use of GREEN-issued Chromebooks in the home. **There are several responsibilities assumed by the parent/legal guardian under this Responsible Use Agreement. These include:**

1. **Sign the Responsible Use Agreement**

2. **Accept Liability**

   The parent/legal guardian and student are responsible for the cost of repairs or the replacement value of the device as of the date of the loss if the property is:

   - Not returned
   - Intentionally damaged
   - Damaged due to negligence
   - Lost or stolen. This must be reported to the School administration immediately. In cases involving theft, a police report will also be required.