

Staff Use of the Internet and Electronic Communications

Acceptable Use Policy

Introduction

Garfield RE-2 School District 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 21st-century technology and communication skills.

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

This Acceptable Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally-owned devices (including, but not limited to, smart phones, computing devices, tablet computers, and all WIFI or data enabled devices) on the school campus.

- The Garfield RE-2 School District network is intended for educational and limited personal use.
- All activity over the network or using district technologies may be monitored 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).
- Misuse of school resources can result in disciplinary action and/or loss of network access.
- Garfield RE-2 School District makes a reasonable effort to ensure 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 IT staff immediately of any concerns for safety or security.

Technologies Covered

Garfield RE-2 School District may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more.

As new technologies emerge that have the potential to enhance the education of students, Garfield RE-2 School District will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

Usage Policies

All technologies provided by the district are intended for educational purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe,

appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Web Access

Garfield RE-2 School District provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow district protocol to alert an IT staff member or submit the site for review from within the block page.

Email

Garfield RE-2 School District provides staff with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school or district policies.

Email accounts should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by district policy.

The district may provide sub-groups within email such as a "Want Ads" group. This group is specifically for staff personal use and is not to be used for business advertising. In addition, items of a dangerous, illegal, or inappropriate manner will not be allowed.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Forwarded, "warning", SPAM, and other "junk" email are a growing problem. Staff should refrain from adding to this problem by sending email of this sort to other staff members. Truly consider whether an email is worth sending on to others before you do it.

Social/Web 2.0 /Collaborative Content

Recognizing the benefits collaboration brings to education, Garfield RE-2 School District may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored.

In addition, there are special guidelines for utilizing Web 2.0 content. Please see the District Social Networking Guidelines for further information.

Mobile Devices Policy

Garfield RE-2 School District may provide users with mobile computers or other devices to promote learning outside of the classroom. Users must abide by the same acceptable 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 your care. Users should report any loss, damage, or malfunction to IT staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse.

Use of school-issued mobile devices off the school network may be monitored and filtered in accordance with district policy and/or CIPA requirements.

Personally-Owned Devices Policy

If a staff member chooses to use a personal Internet connected device on a cellular or other non-district network while on school property, they should exercise caution not to access inappropriate or illegal sites.

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.

If you believe a computer or mobile device you are using might be infected with a virus, please alert IT. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Downloads

You may be able to download file types, such as images, audio, and video. For the security of our network, download such files only from reputable sites, and only for educational purposes.

Netiquette

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

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

Users should also remember not to post anything online that they wouldn't want anyone else to see. Once something is online, it's out there—and can sometimes be shared and spread in ways you never intended.

Plagiarism

Users should not plagiarize (or use as their own, without citing the original creator) content, 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. Research conducted via the Internet should be appropriately cited, giving credit to the original author. This is no

different from credit given to authors work found in other media (such as books, newspapers, or magazines).

Personal Safety

Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't 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 is a crime**. Remember that your activities may be monitored and retained.

Examples of Acceptable Use

Garfield RE-2 staff will:

- Use school technologies for school-related and limited personal activities.
- Follow the same guidelines for respectful, responsible behavior online that they expected to follow offline.
- Treat school resources carefully, and alert IT staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert appropriate personnel if they see threatening, inappropriate, or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places, for primarily educational pursuits.
- Cite sources when using online sites and resources for research.
- Recognize that use of school technologies is a privilege, not a right, and treat it as such.
- Be cautious to protect the safety of themselves and others.
- Help to protect the security of school resources.

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

Examples of Unacceptable Use

Garfield RE-2 staff will not:

- Use school technologies in a way that could be personally or physically harmful.
- Attempt to find inappropriate images or content.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- Access or attempt to access any other users account or files.
- 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 found online.

- Use language online that would be unacceptable 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 their use.

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

Limitation of Liability

Garfield RE-2 School District will not be responsible for damage or harm to persons, files, data, or hardware.

While Garfield RE-2 School District employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

Garfield RE-2 School District will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges
- Disciplinary action up to and including dismissal.
- Legal action and/or prosecution.

If you have questions about this policy, please contact Roger Gose, Garfield RE-2 Director of Instructional Technology.

Adopted: December 12, 2006

Revised: April 24, 2012

LEGAL REFS.: 47 U.S.C. 254(h) (*Children's Internet Protection Act of 2000*)
47 U.S.C. 231 (*Child Online Protection Act of 1998*)
20 U.S.C. 6801 *et seq.* (*Elementary and Secondary Education Act*)
C.R.S. 24-72-204.5 (*monitoring electronic communications*)