

# Parker Unified School District

## Acceptable Use Policy

### Introduction

Parker Unified 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 21<sup>st</sup>-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 all students are expected to follow when using school technologies on the school campus.

- The Parker Unified School District network is intended for educational purposes.
- 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).
- 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.
- Parker Unified School District 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.
- Students who use the district network or other technologies are expected to alert a teacher immediately of any concerns for safety or security.

### Technologies Covered

Parker Unified 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, Parker Unified 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 education purposes. All students 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**

Parker Unified School District provides its students with access to the Internet, including web sites, resources, content, and online tools. That access is restricted in compliance with Children Internet Protection Act (CIPA) regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Students are expected to respect that the web filter is a safety precaution, and should not try to bypass it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the student should follow district protocol to alert a teacher or submit the site for review.

## **Email**

Parker Unified School District **MAY** provide students with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.

If students are provided with email accounts, they should be used with care. Students 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 the district policy or the teacher.

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

## **Social/Web 2.0/Collaborative Content**

Recognizing the benefits collaboration brings to education, Parker Unified School District may provide students with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Students are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Students should be careful not to share personally-identifying information online.

## **Security**

Students 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 you are using might be infected with a virus, please alert a teacher. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

## **Downloads**

Students should **NOT** download or attempt to download or run .exe programs over the school network or onto school resources without express permission from a teacher.

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

## **Netiquette**

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

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

Students should remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's out there—and can sometimes be shared and spread in ways you never intended.

## **Plagiarism**

Students should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Students 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.

## Personal Safety

Students should **NEVER** share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without school teacher permission. Students should recognize there are associated risks with communicating over the internet. Communication carries responsibility for carefully safeguarding the personal information of themselves and others. Students should never agree to meet someone they meet online in real life without parental permission.

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

## Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking 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 can be a crime. Remember that your activities are monitored and retained.

## Examples of Acceptable 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, and 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 myself and others.
- ✓ Help to protect the security of school resources.

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

### **Examples of Unacceptable Use**

I will **not**:

- ✓ Use school technologies in a way that could be personally or physically harmful.
- ✓ Attempt to find, send, store, or display offensive images, pictures, or content.
- ✓ Engage in cyberbullying, hate mail, harassment, insulting or attacking others, discriminatory jokes and remarks.
- ✓ Use school technologies to send spam or chain mail.
- ✓ Violate copyright laws, including plagiarism and downloading of music, video, or program files.
- ✓ Sharing or using others' logons or passwords or other confidential information
- ✓ Provide personal information such as names, addresses, and phone numbers of self or others.
- ✓ Agree to meet someone I meet online in real life.
- ✓ Use language online that would be unacceptable in the classroom, including obscene language.
- ✓ Use school technologies for illegal activities or to pursue information on such activities.
- ✓ Employing the network for commercial or for profit purposes, or for personal gain.
- ✓ Attempting to hack and finding other forms of security breaches that are intentional and directed at harming, destroying, copying, viewing, distributing, modifying or any other alteration to data and software applications that are property of PUSD. In other words, **HACKING** is not allowed. This includes acts that purposely bypass district installed filters, firewalls, anti-virus, or anti-spyware software.
- ✓ Damaging or modifying computers, computer systems or computer networks: downloading installing and using games, audio files, video files or other application including shareware, or freeware without permission to do so.
- ✓ Viewing, modifying, adding, or deleting another person's folders, work or files.
- ✓ Accessing any non-school sanctioned electronic communication such as outside email, chat rooms, social networking sites (FaceBook, My Space, etc.).
- ✓ This is not intended to be an exhaustive list. Students should use their own good judgment when using school technologies.

**Limitation of Liability**

Parker Unified School District will not be responsible for damage or harm to persons, files, data, or hardware.

While PUSD employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

Parker Unified 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, but not limited to:

- Loss of access to the network and Internet resources.
- Notification to parents.
- Disciplinary action including suspension and/or expulsion.
- When applicable, law enforcement agencies will be involved.

**I have read and understood this Acceptable Use Policy and agree to abide by it:**

\_\_\_\_\_  
(Student Printed Name)

\_\_\_\_\_  
(Grade)

\_\_\_\_\_  
(Student Signature)

\_\_\_\_\_  
(Date)

**I have read and discussed this Acceptable Use Policy with my child:**

\_\_\_\_\_  
(Parent Printed Name)

\_\_\_\_\_  
(Parent Signature)

\_\_\_\_\_  
(Date)