

Parker School Acceptable Use Policy

The intent of Parker School's Acceptable Use Policy is to ensure that technology is used in the service of learning, enhancing the educational experience of our students.

Acceptable uses of the technology at Parker School are activities which support teaching and learning. Users are expected to communicate with the same appropriate and courteous conduct online as they would offline or face-to-face, reflecting our core values of excellence, integrity and compassion. They are also encouraged to use technology resources solely for purposes which meet their individual educational needs. Any use of technology that is not in support of educational purposes should be done outside of school hours and without school resources. Violation of the acceptable use policy will result in disciplinary action commensurate to the level of the violation.

Technology includes but is not limited to the school's network, iPads and other tablets, laptops, desktop computers, music listening devices, cell phones and smart-phones.

Unacceptable uses of the network and devices are things which violate the school community and our culture of respect, empathy and unity. Students are expected to show leadership and will be held accountable for unacceptable uses of computers and the network including, but not limited to:

- Accessing Internet resources or visiting websites deemed inappropriate by the staff and administrators of Parker School.
- Inappropriate content in email, messages, documents or online postings.
- Using profanity, obscenity, or other language which may be offensive to another user.
- Using the network for financial gain or for intentionally spreading computer viruses.
- Downloading, storing, or printing graphics, videos, files or messages that are profane, obscene, or that use language that offends or tends to degrade others.
- Taking and/or publishing digital images, audio or videos of other students or employees without their permission.
- Taking and/or publishing digital images, audio or videos that are inappropriate, embarrassing or harassing to other students or employees.
- Intentionally bypassing the Internet filters.
- Violating the privacy rights of students' and employees of Parker School.
- Spamming, sending mass or inappropriate emails.
- Gaining access to other students' accounts, files, and/or data.

Parker School Acceptable Use Policy

- Participation in credit card fraud, electronic forgery or other forms of illegal behavior.
- Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components).
- Transmission of or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients.
- Gaining unauthorized access to computer systems or files.
- Copying print, software, music or video for use in violation of copyright law.
- Attempting to hack into any computer or other device on the school network, or using monitoring software, or keystroke loggers.
- In any manner tampering with technology devices belonging to Parker School or other students.
- Using the Internet to harass or bully fellow Parker students, whether on-campus or off. This includes spreading messages that are hurtful, harassing, sexist, racist or homophobic, via any electronic forum, including but not limited to social networking sites such as Facebook, Formspring, IM, email, blogs, personal websites and video sharing sites such as YouTube. Cyber-bullying is both against Parker School rules and illegal. If you engage in bullying, you will find yourself subject to punishment at Parker School and possibly prosecution by the police.
- Theft. Students are expected to treat their devices in a responsible manner. They should carry their ipads with them at all or times or keep them in their lockers. Outside of Parker, students must protect their belongings and be aware of their surroundings.

The following steps are taken to safeguard employee/student data on our networks:

- Access Controls: Limiting access to authorized personnel only
- Regular Audits: Conducting periodic security audits to identify vulnerabilities
- Training and Awareness: Educating staff on data protection best practices
- Incident Response: Having a robust plan in place to address data breaches promptly

All devices are subject to routine monitoring by teachers and administrators. Parker School technology staff will periodically monitor wireless activity in order to maintain the integrity and security of our network and wireless system. In addition, Parker School reserves the right to confiscate and search all student devices to ensure compliance with the AUP and the Discipline Standards given reasonable suspicion.