



Internet Safety and Acceptable Use Policy

Internet Safety

It is the policy of KIPP Colorado Public Schools to:

- Prevent user access and transmission of inappropriate material via the internet utilizing KIPP technology resources;
- Prevent unauthorized access and other unlawful online activity;
- Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
- Comply with the Federal Communications Commission's Children's Internet Protection Act (CIPA).

This policy applies to all KIPP community members, including students, teachers, staff, and contractual or temporary staff and/or volunteers.

Technology Protection Measure

KIPP Colorado Public Schools shall filter all internet traffic to ensure it is appropriate for minors and in compliance with all local, state, and federal mandates. KIPP Colorado Public Schools shall maintain the necessary licensing to ensure all applicable categories of harmful internet content are blocked and inaccessible by school community members.

Monitoring and Supervision of Online Activities

It will be the responsibility of all members of KIPP Colorado staff to allocate KIPP Colorado technology resources for student use to supervise and monitor appropriate usage of KIPP Colorado technology resources, especially internet access, in accordance with the Children's Internet Protection Act. This includes, but is not limited to:

- In-classroom monitoring of student use of technology resources
- Follow-up meetings with students and/or parents concerning student use of technology resources

KIPP Colorado staff members are responsible for providing instruction to students concerning appropriate online behavior utilizing KIPP Colorado technology resources. Such instruction shall include a review of specific inappropriate behavior, the consequences of such behavior, and an indication of how staff will assist students to be successful with the use of KIPP Colorado technology resources while avoiding inappropriate content. Internet safety education topics include, but are not limited to: online behavior and ethics, social networking safety, chat room safety, cyberbullying awareness and response, and other online privacy and security issues.

KIPP Colorado's network and computing systems are for educational use only. KIPP Colorado makes no assurances of any kind, whether expressed or implied, regarding any internet, network, or electronic communication services. Even with the above provisions, KIPP Colorado cannot guarantee that a student or staff member will not gain access to objectionable or inappropriate internet material. Should any violations occur, the KIPP



Colorado team is committed to acting expeditiously to take corrective action.

Violation of Policy

Any violation or abuse of this policy by KIPP Colorado community members is just cause for taking disciplinary action, up to and including removal of all KIPP Colorado network privileges and accounts, and/or legal action. To keep the KIPP Colorado technology resources and property safe, viable, effective, and user-friendly, all KIPP Colorado community members must work cooperatively and responsibly using this policy. KIPP Colorado reserves the right to update this policy and/or to change the technology protection measure at any time, with or without notice.

KIPP Colorado Acceptable Use Policy

KIPP Colorado will provide members of the school community with access to property and technology resources as necessary and appropriate to fulfill assigned responsibilities. KIPP Colorado community members will not supply personal technology resources to create, store, and communicate organizational information or complete responsibilities, nor will KIPP Colorado support, modify, repair, integrate, or perform work on personal technology resources. Students who are assigned work requiring the use of personal technology resources after-hours away from a KIPP campus are exempt from this requirement.

KIPP Colorado community members who use KIPP Colorado technology resources must do so responsibly, and are required to comply with all state and federal laws, the policies of KIPP Colorado, with standards of professional and personal courtesy and conduct. When using KIPP Colorado property and KIPP Colorado technology resources, the KIPP Colorado community is expected to exercise care, perform required maintenance where assigned, and follow all operating instructions, safety standards, and guidelines. The KIPP Colorado community may not use any technology resource to access, transmit, save, share, or print sexually-explicit images, messages, or any other medium containing such content. In addition, the KIPP Colorado community may not access, transmit, save, share, or print materials that contain ethnic slurs, racial epithets, derogatory, defamatory, obscene or offensive statements or images, or any other content that may be construed as harassing based on someone's race, national origin, sex, gender identity, sexual orientation, physical or mental disability, religious beliefs or any other characteristic protected by federal, state or local laws.

KIPP Colorado's technology resources are to be used by the KIPP Colorado community for the purpose of KIPP Colorado activities. KIPP Colorado does not support the storage and installation of personal hardware or software and related data on KIPP Colorado technology resources. Therefore, KIPP Colorado will not repair or backup such data and software. This includes personal music, videos, pictures, and other documents. KIPP Colorado reserves the right to determine when personal use of technology resources or other KIPP Colorado property is excessive or improper and may require reimbursement or other remediation from a community member and/or discipline the community member when he/she has used the resources excessively or improperly.

The following activities are prohibited while using KIPP Colorado technology resources:

- Knowingly giving one's password to others;



- Attempting to gain unauthorized access to KIPP Colorado technology resources, attempts to disrupt it in any way, or attempts to destroy or alter data;
- Downloading or installing any commercial software, shareware, or freeware without permission from the network administrator;
- Plagiarism;
- Using the organization's time and resources for personal gain;
- Sending or posting discriminatory, harassing, or threatening messages or images;
- Using abusive or otherwise objectionable language in either public or private messages;
- Stealing, using, or disclosing someone else's code or password without authorization;
- Attempting to break into the computer system of another organization or person;
- Accessing, saving, transmitting, or printing any pornographic materials;
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities;
- Using the Internet for political causes or activities, religious activities, or any sort of gambling;
- Changing any computer file that does not belong to the user; and
- Using another person's password without his or her consent.