Internet Safety Policy

KIPP Charlotte’s information technology resources are provided for educational and administrative purposes. The purpose of this policy is to define appropriate use of these resources as we continue to expand their use at KIPP Charlotte in order to enhance educational opportunities. The school system reserves the right to amend this policy at any time and to enforce such amended policy after giving notice of such amendments. The safety of minor children will take precedent over all procedures regarding Internet use.

Technology resources include, but are not limited to, computers, printers, software, personal mobile devices, online catalogs and databases, network file servers, data files, a school-wide e-mail system, access to NCREN, and access to the Internet. KIPP Charlotte’s computer network and Internet access, as well as non-networked access, is available to authorized students, teachers and other staff. The school’s networked resources are protected by a firewall to protect against unauthorized access and use.

There are valuable reasons for using the Internet as an instructional resource at KIPP Charlotte. Accessing local and global information allows the school to enter into partnerships to enhance learning options. Students will broaden problem-solving and decision-making abilities and their research capabilities by using appropriate material, leading to the development of higher level thinking skills. Utilizing the technological devices necessary for Internet access allows students to develop skills for lifelong learning and gain employability skills needed for the 21st century.

It is the intent of KIPP Charlotte to make Internet access available to further the learning of our students. This resource should be used to enhance the curriculum or assist students and staff in meeting their specific educational research needs. Many worldwide resources available on the Internet, however, are not of educational value in a school setting.

In compliance with federal law requirements, an Internet filtering or blocking device is used on all KIPP Charlotte computers that access the Internet. The filter blocks access to three overarching categories of visual depictions of obscene materials, child pornography, and depictions harmful to minors.* KIPP Charlotte acknowledges that even with a filtering system, complete control and/or access to objectionable materials cannot be assured. To address the issue of further controlling access to Internet material, KIPP Charlotte as set the following parameters:

- **Authorized Users** – Only students and employees KIPP Charlotte who complete and sign the technology resource use agreement are authorized users or users of the school’s technology resources.

- **Students and Parents** - The parents or legal guardians of KIPP Charlotte students shall receive and sign an acknowledgment of this Policy and return it to the school. The school shall maintain an accurate record of those who have returned the signed acknowledgment and shall respond accordingly.

- **Technology Privilege** - Use of the KIPP Charlotte’s Internet and technology infrastructure (computers, network file servers, and network wiring) is a privilege, not a right. Inappropriate use will result in an immediate termination of access and other privileges relating to use. Inappropriate use may also result in disciplinary action, up to and including

*See Section 478.02, Florida Statutes, regarding the Children’s Internet Protection Act.
suspension or expulsion for students or formal reprimand or dismissal for staff, as well as potential civil or criminal liability and prosecution. Administration, faculty, or staff may request that the network administrator deny, revoke or suspend specific user access in the event of violation of this policy.

• Violations - Use of technology resources or transmission of any material in violation of any federal or state law is strictly prohibited. Also prohibited are the use or transmission of material protected by federal or state intellectual property laws; copyrighted material; licensed material; threatening, harassing, obscene material and/or pornographic material. In addition, users are prohibited from accessing or attempting to access, using or attempting to use, the Internet or other computer network or non-network facilities for any other unauthorized purposes. This includes but is not limited to commercial activities, introduction of viruses, and manipulation or corruption of systems, files and other related resources. Any illegal activities will be reported to the appropriate agencies. Failure to adhere to KIPP Charlotte’s network policies and rules may subject users to warnings, usage restrictions, disciplinary actions, or legal proceedings.

• Liability – KIPP Charlotte cannot guarantee the availability of technology resources. The school is not responsible for any information that may be lost, damaged, or unavailable due to technical or other difficulties. The school cannot ensure that all electronic transmissions are secure and private and cannot guarantee the accuracy or quality of information obtained. KIPP Charlotte will employ technology protection measures to comply with Federal and State requirements to filter or block material defined to be objectionable. However, no known process can control or censor all illegal, defamatory, or potentially offensive materials that may be available to the user on systems accessible through technology resources in KIPP Charlotte.

All users of KIPP Charlotte technological resources are expected to conduct themselves with respect for others and in accordance with this policy and other school rules governing student conduct. Just as bullying is unacceptable at KIPP Charlotte, so is using an electronic means to cause emotional or physical distress or to interfere with the KIPP Charlotte educational environment. Acts of “cyberbullying” will be dealt with in accordance with the KIPP Charlotte disciplinary guidelines and/or North Carolina law when appropriate.

Cyberbullying actions or communications directed toward any person are prohibited which:

• Occur on, or are delivered to, school property or a school-sponsored activity or event on or off school property; or
• Occur off school property or outside of a school-sponsored activity or event, if the conduct interferes with a student’s educational opportunities or substantially disrupts the orderly operations of the school or school-sponsored activity or event.

Such acts include, but are not limited to:

• Building a fake online profile or website.
• Posting or encouraging others to post on the Internet private, personal, or sexual information.
• Posting a real ”or doctored” image online.
• Accessing, altering or erasing any computer network, computer data, computer program, or computer software, including breaking into a password-protected account or stealing or otherwise accessing passwords.
• Using a computer for "repeated, continuing, or sustained electronic communications, including electronic mail or other transmissions of an unwanted nature.
• Making any statement, whether true or false" that's intended to immediately provoke anyone to "stalk or harass a person.
• Signing up someone for a pornographic website with the intent to intimidate or torment the person.

Users are further prohibited from retaliating against or making false accusations against a victim, witness or anyone else who in good faith provides information about an alleged act of cyberbullying. The School Leader is responsible for implementing this policy, but the responsibilities may be delegated to administrators and others as deemed appropriate.

School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school’s information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

Written complaints regarding student and/or staff access to or use of specific resources available on the Internet will be received, reviewed, and acted upon in accordance with the KIPP Charlotte guidelines for challenged instructional materials.

At any time, parents/guardians may deny their sons/daughters access to the Internet with a written notice to the building principal.

KIPP Charlotte’s Responsibilities

KIPP Charlotte will provide access to technology resources. Users should be aware that use of these resources may be monitored in order to provide an acceptable level of service to all users. Users should also be aware that data that resides on, or passes through, the KIPP Charlotte’s technology infrastructure (computers, network file servers, and network wiring) is subject to review. In order to maintain system integrity and to ensure users are using the system responsibly, school administrators may review files and communications without prior notice or permission of the user. Users should not expect that files stored on district resources will be private.

KIPP Charlotte employs an Internet filter on its network that blocks access to three overarching categories of visual depictions of obscene materials, child pornography, and depictions harmful to minors. Other categories that generally do not provide educational value or promote healthy lifestyles have been blocked from network access as well. The filter that is employed allows flexible configuration so that both categories and individual sites can be blocked. Similarly, the filter can be disabled to allow access specific sites for bona fide research or other lawful purposes.

Although KIPP Charlotte cannot guarantee the accuracy of any information found on the Internet, the staff will provide instruction on proper use of technology resources, including areas of proper care of equipment, management of resources (time and materials), search strategies, user
safety, copyright laws, and computer etiquette. Staff shall report any incident of harassment or any other unauthorized or inappropriate use of school division technology resources to the building or department administrator who will report the incident to school administrators.

KIPP Charlotte teachers will supervise and model appropriate use of the Internet. Students will continue to have Internet access under direct teacher supervision; however, students will, also, experience guided practice leading towards gaining skills to become an independent, responsible user of the Internet. Teachers will model skills needed to search for information within an area of study, to filter information for credibility and worth, and to recognize areas of inappropriate information sources or access. Teachers will explore an Internet site before directing students to that site. Teachers will make every effort to ensure that students are directed only to sites with age- and topic-appropriate material and resources. Teachers will make every effort to ensure that students explore only sites with age- and topic-appropriate material and resources.

The school division will provide access to electronic mail for all staff members. Students will not be issued individual e-mail accounts. In the event that a teacher maintains a supervised class account, the teacher will maintain security of the class account password and will directly supervise individual student use of the account. Students who have electronic mail accounts from sources outside the school division may not access those accounts using the school division's resources.

The KIPP Charlotte Development Office controls access to and information provided on the corporate website, www.kippcharlotte.org. When authorized, other staff members may post information to the Student and Family Assistant page of the site (the parent portal.) Parents and guardians are provided read-only access to the information and cannot post materials or make comments on the site.

User Responsibilities

All users will only use technology for school-related purposes in a responsible, ethical, and legal manner. Users should not access, modify, or destroy other user's data without appropriate authorization. Users should not knowingly spread a computer virus, impersonate another user, violate copyright laws, download, install or use unauthorized software, including music or video files, damage or destroy resources, or intentionally offend, harass, or intimidate others.

All users will view sites that directly relate to a school-related assignment, activity, or responsibility. Users should not use school technology resources to create, distribute, download, or view obscene, threatening, illegal, or inappropriate content. Users should immediately inform a school administrator if they encounter material that is obscene, illegal, inappropriate, offensive, or otherwise makes them feel uncomfortable.

Users will use resources responsibly. Users will not give out passwords. Users should not disrupt network usage by others, monopolize technology resources, print excessively, nor use excessive amounts of shared data storage space. Users may not use the network for financial gain, commercial or political activity or illegal acts such as hacking. Users may not access the network through wireless systems without permission from KIPP Charlotte.
Students should not use technology resources to engage in any commercial activity including the purchase of goods and services. Staff members may use technology resources to purchase school supplies and resources provided they follow established KIPP Charlotte purchasing guidelines.

Staff members may not abuse their access to technology resources. Abuse may consist of excessive or unacceptable use. A use is unacceptable if it conflicts with KIPP Charlotte's purpose, goal, or mission or with a staff member’s authorized job duties or responsibilities.

Date Approved: October 27, 2011  
Date Amended: December 1, 2012

Date Retired

* OBSCENE, as that term, is defined in section 1460 of title 18, United States Code. CHILD PORNOGRAPHY, as that term, is defined in section 2256 of title 18, United States Code. HARMFUL TO MINORS means any picture, image, graphic image file, or other visual depiction that:
1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

SEXUAL ACT and SEXUAL CONTACT have the meanings given such terms in section 2246 of title 18, United States Code.

MINOR, for the purposes of this document, means any individual who has not attained the age of 17 years.