STUDENT/ALUMNI CYBER SAFETY

KIPP SoCal's Position on Student/Alumni Cyber Safety

The safety of our students, alumni, families, and team members is a priority of KIPP SoCal Public Schools ("KIPP SoCal"). The Internet and other online programs and resources are to be utilized by our students, alumni, families, and team members to support instructional programs and appropriate virtual student learning and messaging. While the Internet can be a powerful educational tool, it is also an unregulated space that contains materials, social media activity, and negative and abusive messaging unsuited to the school setting. For this reason, KIPP SoCal Public Schools ("KIPP SoCal") will make every reasonable effort to ensure that the resources and programs that we provide are monitored to ensure they are used responsibly. KIPP SoCal Public Schools will comply with the requirements of the Children's Internet Protection Act (CIPA) and is committed to assuring the safe conduct and well being of students/alumni while online.

Students and families have been notified about authorized uses, obligations, and responsibilities for users of KIPP SoCal Chromebooks, other devices, and technology as well as consequences for unauthorized use and/or unlawful activities in accordance with KIPP SoCal's regulations and KIPP SoCal's Student and Family Acceptable Internet Use Policy.

KIPP SoCal reserves the right to monitor the use of technological resources, including the Internet and email, for audit and review purposes. Users should not have an expectation of privacy when using KIPP SoCal technology resources.

KIPP SoCal will ensure that all KIPP SoCal Chromebooks and any other devices with Internet access have a technology protection measure through our web filtering system that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors and that the operation of such measures is enforced. (20 U.S.C. 6777, 47 U.S.C. 254). Students may not access prohibited materials at any time, for any purpose. This includes material that is obscene, child pornography, or material that is considered harmful to students, as defined by the Children's Internet Protection Act, which aims to protect children from obscene or harmful content on the Internet.

The Children's Internet Protection Act (CIPA) defines "harmful to minors" to mean: any picture, image, graphic image file, or other visual depiction that - (i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (ii) 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 (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors. (47 U.S.C. 254(h)(7)(G)).

Students/alumni shall not disclose personal information about themselves or others on the Internet or other resources. For example, students/alumni shall not reveal their name, home address, telephone number, or display images of themselves or others.

KIPP SoCal Team Member Guidelines for Interactions with Students and Alumni Online and Other Media (such as phone calls, text messages, etc.)

As stated in the Team Member Handbook, all KIPP SoCal team members are held to the highest standard of professionalism with our students, alumni, families, alumni, and other team members. Our Professionalism policy states, "KIPP SoCal is a professional organization based on the trust and goodwill it engenders from its community. In addition to providing excellent services to the communities in which we serve, you are to treat all families, colleagues and stakeholders with the utmost courtesy."

All team members are expected to remain professional while communicating with students and families online and other media, such as phone calls, text messages, etc. Our focus should always be concerned for these three reasons: *for student/alumni's education, health, and safety.*

The following are guidelines for all communications:

- All team members are expected to stay within professional boundaries with students and alumni
    - As stated in the Team Member Handbook, all team members are expected to conduct themselves in a way that reflects the highest standards of behavior and professionalism required of team members.
    - It is each team member's obligation to avoid situations that could prompt suspicion by families, students, alumni, colleagues, or school leaders.
        - Some activities may seem innocent from a team member's perspective, but can be perceived as flirtation, sexual insinuation, or unprofessional from a student, alumni, or family's point of view.
            - This is not to restrain innocent, positive relationships between team members and students, but to prevent interactions that could lead to, or may be perceived as, unprofessional.

- Keep the conversation related to the education process (as stated in Use of Electronic Media by Team Members to Communicate with KIPPsters policy found in the Team Member Handbook)
    - We do encourage team members to check in with students, alumni, and families to see how they are doing
        - If the student/alumni and/or family ask for assistance with resources, please let them know we are here to assist and we will provide assistance

as much as we can or provide information on other resources that may be available.
        - Please try **not** to probe the student/alumni and/or family about something personal that they are not comfortable speaking about.
            - Allow the family to speak on these things on their own.

- Keep the conversation professional in tone, words used, and focus
    - Please refrain from putting long conversations in emails and texts
        - These conversations should be done by phone

- Keep the families included in communications with students

- Keep your conversations with students/alumni and families on KIPP SoCal authorized means of communication
    - Use your KIPP SoCal issued phone, email address, and any other KIPP SoCal authorized virtual communication resource, such as Google Classroom, Class Dojo, etc.

- Refrain from using personal social media accounts to communicate with students/alumni and families

<u>Online Threats to Students/Alumni</u>

As well as the threats that all users face when going online, such as computer viruses and email scams, students/alumni are at risk from the following:

- *Cyberbullying*
    - Bullying that takes place over digital devices such as cell phones, computers, and tablets. Cyberbullying can occur through SMS, text, and mobile applications (apps) or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else, causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behavior.

- *Inappropriate Content*
    - Adolescents and children can unintentionally come into contact with inappropriate content, such as sexually explicit material. Unsolicited obscene materials can also be received electronically.

- *Sexting*
    - Sexting is the sharing and receiving of sexually explicit messages and nude or partially nude images via text messages or apps. Sexting, while commonly occurring off school grounds, also occurs on school property, with the content

being sent and viewed on cell phones. Of note is that possession of sexually explicit photos received by sexting can be considered a type of possession of child pornography from a legal perspective.

- *Sextortion/Ransomware*
    - Students may also become victim to sextortion, possibly via ransomware, if they engage in sexting. Sextortion occurs when someone threatens to distribute private and sensitive material if not provided with images of a sexual nature, sexual favors, or money. Ransomware is a particular form of computer malware in which perpetrators encrypt users' files, then demand the payment of a ransom for users to regain access to their data. Ransomware can also include an element of extortion, in which the perpetrator threatens to publish data or (possibly sexually explicit) images if the victim does not do what the perpetrator wants, such as provide nude photos.

- *Oversharing*
    - Personal information that is sometimes shared by students includes their name, age, address, phone number, and Social Security number. • Online Predation. Online predators put victims through "the grooming process," a series of steps by which they build the victim's trust by sympathizing with him or her or feigning common interests, after which they proceed to set up a face-to-face meeting with the victim and then move forward with manipulation and seduction.

Additional Resources for Students, Families, Alumni, and Team Members

Students, alumni, team members, and families can receive additional guidance on online safety through the following:

General Education on Online Safety

- *Stop.Think.Connect.* Campaign (https://www.dhs.gov/stopthinkconnect; U.S. Department of Homeland Security) is a national awareness campaign that provides resources such as videos, a toolkit, and blogs to help raise the awareness of cyber threats and how to be safer online.

- *NetSmartz® Workshop* (https://www.netsmartz.org/; *National Center for Missing and Exploited Children® [NCMEC])* provides resources for parents and guardians, educators, and law enforcement with the goal of educating, engaging, and empowering children to recognize potential Internet threats, talk to adults about risks, prevent themselves from being exploited, and report victimization to adults. Separate Websites and resources are available for kids, tweens, and teens.

- *OnGuard Online program* https://www.consumer.ftc.gov/features/feature-0038-onguardonline; Federal Trade Commission) provides instructional material for elementary and middle school teachers,

high school teachers, and community educators and resources for parents on how to talk to their children about being online.

- *Incorporating Sextortion Prevention, Response, and Recovery into School Emergency Operations Plans (EOPs) Webinar, REMS TA Center*. This Webinar provided background information on sextortion and discussed how students/alumni can be victims and perpetrators. Presenters shared how education agencies can develop measures to prevent and protect students/alumni from sextortion with support from local and Federal agencies. http://rems.ed.gov/Sextortion2016Webinar.aspx

- *Office of Educational Technology (OET) Web page, U.S. Department of Education*. The OET develops national educational technology strategy and policy for how technology can be used by K-12, higher education, and adult education learners. https://tech.ed.gov/

- *Privacy Technical Assistance Center, U.S. Department of Education*. This Website serves as a comprehensive resource that education agencies can use to get information about privacy, confidentiality, and security practices. The site provides valuable information related to information sharing guidelines, such as the Family Educational Rights and Privacy Act (FERPA), and legislation, such as the Children's Internet Protection Act. http://tech.ed.gov/privacy

- *StopBullying.gov Website*. This Website (http://www.stopbullying.gov/index.html) serves as a hub of information on the Federal perspective on bullying and contains information and resources to address bullying. Under the Cyberbullying tab, users can access Web pages such as: o Tips for Teachers, which describes some of the warning signs that a child may be involved in cyberbullying and how to prevent and address cyberbullying; and o Social Media and Gaming, which lists social media apps and sites commonly used by children and teens and what adults can do to prevent cyberbullying of children who are gaming.

After an Online Incident has Occurred

Students/alumni also need to be aware of what to do if they are a victim of an online threat. They are encouraged to report threats to their parent/guardian, a teacher, a school counselor, another trusted adult, and the online service provider, if appropriate. Students, alumni, teachers, and other members of the public can also contact NCMEC's CyberTipline to report a concern by submitting an online report at https://report.cybertip.org/ or calling 1-800-843-5678.

If somebody is in immediate danger or a crime may have been committed, students, teachers, and team members should contact local law enforcement.