Student Technology Acceptable Use Policy

Educational Technology- Terms and Conditions

The administration or designated representatives will provide age-appropriate training for students who use Kelloggsville Public Schools educational technology. The training provided will be designed to promote Kelloggsville Public Schools commitment to:

- The standards and acceptable use of Internet services as set forth in the Kelloggsville Public Schools Internet Safety Policy;
- Student safety with regard to:safety on the Internet; appropriate behavior while on online, on social networking Web sites, and in chat rooms; and cyberbullying awareness and response.
- Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Acceptable Use - The use of educational technology must be in support of education and research and consistent with the educational objectives of Kelloggsville Public Schools. The use of Kelloggsville Schools educational technology is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The following prohibitions apply to all users:

1) **Major Offenses**-

No user shall:

a) Access, transmit, or retransmit material which promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacture of destructive devices such as explosives, fireworks, smoke bombs, incendiary devices or the like;

b) Commit or attempt to commit any willful act involving the use of the network which disrupts the operation of the network within the school district or any network connected to the Internet including the use or attempted use or possession of computer viruses.

c) Sending, sharing, viewing, or possessing pictures, text messages, e-mails, or other materials of a sexual nature (i.e. sexting) in electronic or any other form, including the contents of a personal communication device or other electronic equipment. Such actions will be reported to local law enforcement and child services as required by law.

d) Use of Education Technology to access, process, distribute, display or print child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors is prohibited. Offensive messages and pictures, inappropriate text files, or files dangerous to the integrity of the District's computers/network (e.g., viruses) are also prohibited.

e) Access, transmit, or retransmit material which advocates or promotes violence or hatred against particular individuals or groups of individuals or advocates or promotes the superiority of one racial, ethnic or religious group over another;

f) Harass, intimidate, threaten, bully, or abuse any person or entity, by any means, including the use of vulgar, hateful, racially or ethnically offensive, sexually harassing, or otherwise objectionable content. Use of the educational technology to engage in cyberbullying is prohibited. "Cyberbullying" is defined as the use of information and

communication technologies (such as email, cell phone and pager text messages, instant messaging (IM), defamatory personal websites, and defamatory online personal polling websites), to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others." Cyberbullying includes, but is not limited to the following:

1) posting slurs or rumors or other disparaging remarks about a student on a website or on weblog;
2) sending e-mail or instant messages that are mean or threatening, or so numerous as to drive up the victim's cell phone bill;
3) using a camera phone to take and send embarrassing and/or sexually explicit photographs/recordings of students;
4) posting misleading or fake photographs of students on websites.

g) Access, transmit, or retransmit material which violates state or federal law;
h) Use or possess “bootleg software” (“bootleg software” means any software which has been downloaded or is otherwise in the user’s possession without the appropriate and lawful registration of the software including the payment of any fees owing to the owner of the software);
i) Attempt to log on to educational technology as a system administrator, or any access level other than granted
j) Vandalize networks, hardware or software through alterations, damage, denial of service, port scanning, or other means.
k) Use or possess any software used to illegally access computers, servers or networks, perform scanning of computers, servers or networks, or circumvent the Internet content filters. This includes, but is not limited to, any software or scripts commonly accepted as “hacking software.”
l) Use or possess any device that provides wireless Internet access other than those devices provided by Kelloggsville Public Schools.
m) Use of another person's account/email address/password is prohibited. Students may not allow other users to utilize their account/email address/password. Students may not go beyond their authorized access. Students are responsible for taking steps to prevent unauthorized access to their accounts by logging off or "locking" their computers/laptops/tablets/personal communication devices when leaving them unattended;
n) Attempt to hide the origin of network communications through software or hardware anonymous or pseudonymous connections.
o) Attempt to subvert content filters designed to prevent access to undesirable content. (e.g. online proxies)

Consequences: Are clearly defined in the Kelloggsville Virtual School Continuum of Expectations (Secondary version) located at the end of this document.

2) Minor Offenses-

No user shall:

a) Use encryption software from any access point from within the school district;
b) Transmit credit card information or other personal information from an access point from within the school district;
c) Download and/or install any programs including, but not limited to, games or instant messaging programs except for specific files essential to educational instruction.

d) Download copyrighted files including, but not limited to, audio or video except for specific files essential to educational instruction.
e) Post personal or private student information using District educational technology without consent.
f) Use vulgarities or other inappropriate language.
g) Accessing or participating in online "chat rooms" or other forms of direct electronic communication (other than e-mail) without prior approval from a teacher, administrator, or the Director of Technology. All such authorized communications must comply with these guidelines. Students may only use their school-assigned accounts/email addresses when accessing, using or participating in real-time electronic communications for education purposes
h) Modify or remove the KPS asset tab, vendor asset tab, or the manufacturer serial number and model number tag.

Consequences: Are clearly defined in the Kelloggsville Virtual Continuum of Expectations (Secondary Version) located at the end of this document.

3) Chromebook Guidelines-

In addition to the specific requirements and restrictions detailed above, it is expected that students and families will apply common sense to the care and maintenance of district-provided chromebook. In order to keep devices secure and damage free, please follow these additional guidelines.

a) You are responsible for the device, charger, cords, school-owned case, etc. Do not loan any of these items to anyone else.
b) While a properly designed case affords some protection, there are still many fragile components that can easily be damaged by dropping, twisting or crushing the device.
c) Do not eat or drink while using the chromebook or have food or drinks in close proximity. Any liquid spilled on the device may very well cause damage (often irreparable) to the device.
d) Keep your chromebook away from precarious locations like table edges, floors, seats or around pets.
e) Do not stack objects on top of your chromebook; leave outside or use near water such as a pool.
f) Devices should not be left in vehicles. Devices should not be exposed to extreme temperatures (hot or cold) or inclement weather (rain, snow).
g) Do not store or transport papers or other objects between the screen and keyboard.

4) Computer Damages-

If a computer is damaged, the school must be notified immediately. If a student damages a chromebook due to negligence, the student/student's family is responsible for paying repair costs according to the repair costs determined by KPS up to the full cost of a replacement device. KPS reserves the right to charge the student and guardian the full cost for repair or replacement when damage occurs due to negligence as determined by the administration. Examples of negligence include, but are not limited to:

a) Leaving equipment unattended and unsecured. This includes damage or loss resulting from an unattended and unsecured device at school.
b) Lending equipment to others other than one's parents/guardians.
c) Using equipment in an unsafe manner or environment.

d) Ignoring common sense guidelines delineated above.
e) A student who does not have a chromebook due to it being damaged may be allowed to use a chromebook while attending the academic help room at school depending on availability and reason for loss. Students whose chromebook has been damaged due to negligence may not be allowed to take the loaner chromebook home for the remainder of the year or until such time that they demonstrate the ability to properly care for the device as determined by administration.
f) If the device charger is damaged or lost, the student is responsible for the cost of replacing it.
g) Access to a KPS provided chromebook and network should be considered a privilege that must be earned and kept. A student's technology privileges may be suspended due to negligent damage to the device, or inappropriate use of the device that fails to comply with the KPS technology agreements outlined in this document.

5) Theft or Loss of Equipment-

a) Incidents of theft must be reported to the police by the parent/guardian and a copy of the police report must be given to the principal or the building administrator within 48 hours. Students who fail to do so are responsible for the replacement cost of the device. Any theft occurring on school grounds must be reported immediately to a building administrator. The principal will then file a police report.
b) If there is no evidence of theft, or if the chromebook has been lost due to a student's negligence, the student will be responsible for the chromebooks replacement cost.

6) Online Etiquette-

a) Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through the district's education technology. Do not use obscene, profane, vulgar, sexually explicit, defamatory, or abusive language in your messages.;
b) Never reveal names, addresses, phone numbers, or passwords of yourself or other students, family members, teachers, administrators, or other staff members while communicating on the district's education technology;
c) Do not transmit pictures or other information that could be used to establish your identity without prior approval of a teacher;
d) Never agree to get together with someone you "meet" on-line without prior parent approval.
e) Students should promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable, especially any e-mail that contains sexually explicit content (e.g. pornography). Students should not delete such messages until instructed to do so by a staff member.

7) Preservation of Resources and Priorities of Use:

Computer resources are limited. Because space on disk drives and bandwidth across the lines which connect the District's Ed-Tech (both internally and externally) are limited, neither programs nor information may be stored on the system without the permission of the Director of Technology. Each student is permitted reasonable space to store e-mail, web, and personal files. The Board reserves the right to require the purging of files in order to regain disk space. The following hierarchy will prevail in governing access to the Ed-Tech:

a) Class work, assigned and supervised by a staff member;
b) Personal correspondence (e-mail–checking, composing, and sending);

c) Training (use of such programs as typing tutors, etc.);
d) Personal discovery (“surfing the Internet”);
e) Other uses – access to resources for “other uses” may be further limited during the school day at the discretion of administration.

Privacy in communication over the Internet and through the district's education technology is not guaranteed. To ensure compliance with these guidelines, the district reserves the right to monitor, review, and inspect any directories, files and/or messages residing on or sent using the district's education technology. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

Users have no right or expectation to privacy when using the education technology. The district reserves the right to access and inspect any facet of the education technology, including, but not limited to, computers, chromebooks, tablets, personal communication devices, networks or Internet connections, online educational services, e-mail or other messaging or communication systems or any other electronic media within its technology systems or that otherwise constitutes its property and any data, information, e-mail, communication, transmission, upload, download, message or material of any nature or medium that may be contained therein.

A student's use of the education technology constitutes his/her waiver of any right to privacy in anything s/he creates, stores, sends, transmits, uploads, downloads or receives on or through the education technology and related storage medium and equipment.

Routine maintenance and monitoring, utilizing both technical monitoring systems and staff monitoring, may lead to discovery that a user has violated Board policy and/or the law. An individual search will be conducted if there is reasonable suspicion that a user has violated Board policy and/or law, or if requested by local, State or Federal law enforcement officials. Students’ parents or legal guardians have the right to request to see the contents of their children’s files, e-mails and records.

The Kelloggsville Public School District makes no warranties of any kind, whether expressed or implied, for the service it is providing. Kelloggsville Public School District will not be responsible for any damages you suffer. All communications and information accessible via the network should be assumed to be property of Kelloggsville Public Schools.

Use of any information obtained via the Internet is at your own risk. The Kelloggsville Public School District specifically denies any responsibility for the accuracy or quality of information obtained through its services

ACKNOWLEDGEMENT OF RECEIPT
AND AGREEMENT TO ABIDE BY THE
KVS Student Handbook
and
Student Technology Acceptable Use Policy

Each student will be required to sign this form to acknowledge that they have received their handbook. This form must be completed prior to starting the students learning experience with Kelloggsville Virtual School. It is the student's responsibility to be familiar with the contents of this handbook. Students are encouraged to share this handbook with their parents and/or guardians.

By signing this form I acknowledge the following:

1. I have read this **handbook** and understand its contents.

2. I also understand and will abide by the **Internet/Network Acceptable Use Policy**.

_____ _____
Student Name (print) **Grade**

_____ _____
Student Signature **Date**

_____ _____
Parent Signature **Date**