

Responsible Use of Technology

Introduction

Kane School District provides technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence within Kane School District by facilitating resource sharing, innovation and communication with the support and supervision of parents, teachers and support staff. Other appropriate educational uses of these resources include, but are not limited to, classroom-based projects and student works, college and career explorations, and high-quality, academically-enriching research. The use of these technology resources is a privilege, not a right.

With access to many different technology resources and people from all over the world, there comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. Kane School District firmly believes that the value of information, interaction, and research capabilities available (including, but not limited to, email, the Internet, and social media) outweighs the possibility that users may obtain material that is not consistent with the educational goals of Kane School District.

Proper behavior, as it relates to the use of technology resources, is no different than proper behavior in all other aspects of Kane School District activities. Recognizing the value of the Internet, Kane School District supports teachers, students, all Kane School District personnel and any school or district guests being engaged in an online environment that allows them to discuss, collaborate, communicate, create, and share in a safe, ethical, and responsible manner. This expectation extends to all Kane School District technology resources, as well as personal networks and devices inside and out of the school. This document is intended to clarify those expectations as they apply to technology resource usage and is consistent with Kane School District policy.

Kane School District will provide school-wide and/or classroom training for employees and students according to current Utah State Board of Education (USBE) Rules.

Responsible Use

This Responsible Use for Technology Resources Policy is to prevent unauthorized access and other unlawful or improper activities by users online, prevent unauthorized disclosure or access to sensitive or confidential information, ensure responsible and appropriate use of its technology resources, and to comply with the [Child's Internet Protection Act \(CIPA\)](#). As used in this policy, "user" includes anyone using Kane School District technology resources, including computers, Internet, email, chat rooms, wireless network, and other forms of direct electronic communications or equipment provided by Kane School District. Only current students, employees, officers, volunteers, substitutes and authorized visitors of Kane School District are permitted to use Kane School District technology resources and network.

Students who are under 18 must have their parent(s) or guardian(s) authorize student use of Kane School District technology resources and acknowledge compliance with this policy. Students who are 18 or older, as well as employees and other users, must acknowledge their compliance with this policy, either electronically online or by signing and returning a copy of the acknowledgement form provided below. **The absence of a signed acknowledgment does not excuse compliance with this policy. All users must follow this policy and report any misuses of Kane School District technology resources to a teacher, supervisor, administrator, or appropriate Kane School District personnel.** By using Kane School District technology resources, users are held to have agreed to comply with this policy. If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult Kane School District personnel in advance of any questionable use.

Disciplinary Actions due to Violations of this Responsible Use Policy

Violation of this Responsible Use policy, or other device, technology or Internet policies, rules, or agreements may result in the user's access being suspended or having access completely revoked. Students violating the district Responsible Use Policy will be subject to the following punishments:

Minor Violations:

1. Loss of computer privileges or Internet access rights.

A. First offense: verbal warning and/or loss of Internet access for up to one week as directed by principal.

B. Subsequent offense for same violation: Loss of Internet privilege for a period exceeding one week as directed by principal.

More Serious Violations:

1. Suspension of Internet or network access for any period exceeding one month;

2. Revocation of Internet or network access;

3. Referral to legal authorities;

4. Suspension from school;

5. Loss of employment (if a staff or faculty member);

6. Referral to State Professional Practices Board (if a staff or faculty member).

- **Violations of the acceptable use policies that may result in confiscation of LEA-owned electronic devices or restricted access on the LEA's network**
- **Use of electronic devices in violation of an LEA's or teacher's instructional policies may result in the confiscation of privately-owned electronic devices for a designated period; and**
- **Uses of privately-owned electronic devices to bully or harass other students or employees during school hours or at school-sponsored activities may result in the student being subject to LEA disciplinary action**
- **Any misuse if appropriate may be reported to law enforcement**
- **Misuse by employees may result in criminal and/or employment consequences**

The use of any technology resource (including, but not limited to, desktop computers, mobile devices, personal/Kane School District devices, network-delivered services, the Internet, audio-visual equipment, digital content and social media) must support the educational goals of Kane School District. Use must be authorized by a Kane School District staff member and must lie within the bounds of Kane School District curriculum and educational purpose.

When placing, removing, or restricting access to specific databases, the Internet and/or any other technology resource, school officials shall apply the same criteria for educational suitability used to evaluate all other educational resources.

Responsible uses of Kane School District's network and technology include:

- a. Searching for and accessing appropriate information and materials. The material you access through Kane School District's network system should be for class assignments or for research on subjects similar to what you might study in a class or in the school library.
- b. Using school technology resources to do homework, write papers, and create presentations, videos and movies, and other creative projects. Make sure that the work that you turn in is yours and do not plagiarize works that you find on the Internet. Plagiarism is taking the ideas, graphics, or writings of others and presenting them as if they were yours without adequate and accurate citation.

- c. You own the copyright to works that you create in school or for a class assignment. If the work is created by a group, each student will share joint ownership of the copyright. You and your parent or guardian must agree before your work will be posted on the school or Kane School District Web site. Your work should be posted with your copyright notice.
- d. Accessing social media sites like Facebook, YouTube & Twitter is allowed only by permission as a part of a class assignment or project. Accessing social media for entertainment purposes is not allowed.
- e. Taking appropriate photos & video with a Kane School District or personal device of classroom or school activities or other public school areas is allowed and encouraged. Be sure to get permission from your teacher, the school, and each individual in a photo or video before posting or sharing online.
- f. Respect the rights of copyright owners in your use of materials found on, disseminated through, or posted to the Internet. Copyright infringement occurs when you reproduce a work that is protected by a copyright without explicit permission from the copyright holder or outside the limitations of copyright law. Do not use peer-to-peer file sharing programs, such as "BitTorrent" or "Limewire," to download or share copyrighted movies, music, or games.
- g. Be considerate of your Internet and network usage. In times of high use, refrain from streaming music & video, and postpone downloading large files to a time when network use is low. Delete your download files when you are done with them or when you log off of a Kane School District device.
- h. If you mistakenly access inappropriate information, you should immediately report this access to a teacher or an administrator. **This will protect you against a claim that you have intentionally violated this policy.**
- i. Kane School District has taken reasonable steps to restrict access to materials it considers harmful and to materials that do not support or conform to accepted educational objectives. These steps include Kane School District installing filtering software & hardware to protect against access to inappropriate material in accordance with the [Children's Internet Protection Act \(CIPA\)](#). If you feel that the filtering software is blocking your access to an appropriate site, report this to your school librarian, computer lab coordinator, teacher, or an administrator.
- j. Do not share your personal contact information with anyone you don't know and trust personally. This includes your full name, together with other information that would allow an individual to locate you, including your family name, your home address or location, your work address or location, or your phone number. You may disclose personal contact information to educational institutions, companies or other entities for college/career exploration purposes, or with specific staff approval.
- k. Protect the personal contact information of others. You will not disclose names or any other private or personal information about other students. You will not forward a message that was sent to you privately without permission of the person who sent you the message.
- l. You will promptly disclose to your teacher or other school staff any message you receive that is inappropriate or makes you feel uncomfortable. You should not delete such messages until instructed to do so by a staff member.
- m. Your parents and authorized district personnel have the right to request to see the contents of your computer or device files at any time.
- n. If you want or need to use a Web browser extension or add-on, please ask your teacher or local technology support person for permission to add or install it.
- o. If you observe someone using school technology in an inappropriate manner, you will report it to an adult as soon as possible, even if it is done anonymously.
- p. Part of being a good digital citizen is understanding the individual environment you are in. Follow the different rules and expectations of each teacher or administrator.

Inappropriate Uses

Individual(s) involved in any of the following will be subject to disciplinary or corrective action in accordance with applicable Kane School District policy, handbooks, rules and regulations:

- a. Possessing, accessing, transmitting, copying, or creating material that violates the Student Code of Conduct, Kane School District policy, student or employee handbooks, or Kane School District rules and regulations, including but not limited to content that is inappropriate, illegal, copyrighted, pornographic or obscene, stolen, threatening, discriminatory, harassing, or offensive
- b. Attempts to bypass or disable Kane School District Internet filter, security systems or software
- c. Attempts to access, alter, interfere with, damage, or change network configuration, security, passwords, or individual accounts of another without written permission from Kane School District Technology Department
- d. Any unauthorized attempts to circumvent passwords or obtain access to passwords or other security-related information
- e. Disclosing any other user's password to others or allowing another individual to use another's system account
- f. Attempts to upload, create, or transmit computer viruses
- g. Attempts to access or install unlicensed, inappropriate, or unapproved software or technology
- h. Attempts to alter, disconnect, destroy, hack, or disable Kane School District computer equipment, mice, keyboards or other computer components, personal/Kane School District devices, Kane School District data, the data of others, or other networks connected to Kane School District system, including while off school property
- i. Plagiarism or use of Kane School District technology resources to engage in academic dishonesty
- j. Use of Kane School District technology resources and devices at anytime and in any place to access, create, send or post material that is obscene; child pornography; material that depicts, or describes in an offensive way, violence, nudity, sex, death, or bodily functions; material that has been designated as for adults only; material that promotes or advocates illegal activities; material that promotes the use of alcohol or tobacco, school cheating, or weapons; or material that advocates participation in hate groups or other potentially dangerous groups
- k. Unauthorized use of any Kane School District technology resource or personal/Kane School District device for non-educational purposes or outside the bounds of Kane School District curriculum
- l. Use of email, the Internet, or social media resources at school to engage in conduct that violates the Student Code of Conduct or threatens school safety
- m. Use of Kane School District technology resources, including email, the Internet or social media resources to threaten, harass, bully, retaliate, discriminate against other students, employees, guests or volunteers
- n. Use of personal email, the Internet, or social media resources, without regard to whether it occurs on school property, to engage in conduct that involves a public school and contains the elements of the offense of terroristic threat or false alarm, or otherwise causes a substantial disruption to the educational environment
- o. Violating or infringing upon the intellectual property, copyrighted or trademarked rights of another
- p. Using Kane School District's network system for personal commercial purposes. You may not offer, provide, or purchase products or services without authorization through Kane School District's network system.
- q. Possessing, accessing or transmitting any material, which is considered inappropriate or is in violation of any local, state or federal law is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secrets

These are examples of inappropriate conduct that would violate this policy. Kane School District reserves the right to take immediate disciplinary or corrective action against a user that engages in conduct that: (i) creates security or safety issues for Kane School District, students, employees, schools, networks, or technology resources, or (ii) is determined to be inappropriate or inconsistent with Kane School District policy or law.

Personal Electronic Devices

Kane School District will allow students to use personal electronic devices to access Kane School District wireless network in all schools. This wireless access provided to the devices is designed to enhance the students' educational experience and outcomes. Connecting to Kane School District Wi-Fi network with personal devices is a privilege, not a right, and is strongly recommended for students since our network is filtered and monitored for inappropriate use. Permission to bring and use personal devices is contingent upon adherence to Kane School District guidelines. If a personal device is used by a student to disrupt the educational environment, in the sole opinion of Kane School District, that student's privileges may be limited or revoked.

If a teacher allows the use of a personal electronic device in the classroom, they will clearly communicate to parents and students the conditions under which the use of a personal electronic device is allowed.

General Guideline and Rules

1. All students may use a personal electronic "Internet ready" device on Kane School District wireless network by completing and submitting the attached Personal Electronic Device Policy Agreement to the main office
2. The use of the personal electronic device is solely limited to support and enhance instructional activities currently occurring in the classroom environment.
3. Recognizing that all such devices may not be appropriate for instructional situations, personal electronic devices will be considered for classroom use if they are mobile and have the capability of browsing the Internet. These items include, but are not limited to: laptops, netbooks, tablets, cell phones, e-readers and handheld gaming devices. The final determination of devices that are appropriate to connect to Kane School District network rests with the school administration.
4. Students are discouraged from accessing the Internet using private LTE or any high bandwidth external network subscriptions through their own Internet Service Provider.
5. Connecting a personal electronic device may not be successful if the technical specifications for wireless protocol are not met.
6. No personal electronic device may be connected to any Kane School District network if a signed AUP/RUP and Personal Electronic Device policy form are not on file in Kane School District student information system.
7. All information related to the personal electronic device(s) that is requested by this form will be submitted by the student prior to accessing the network.
8. No student shall establish a wireless ad-hoc or peer-to-peer network using his/her electronic device or any other wireless device while on school grounds. This includes, but is not limited to using a personal electronic device as a cabled or wireless hotspot. Example: Using a personal device as a server so that students can play an online game.
9. Network access is provided via Wi-Fi / wireless connection only. No one is allowed to connect a personal electronic device to the network by an Ethernet cable plugged into a data jack in the school. Violation of this term will result in disciplinary action and revocation of access to the network.
10. Teacher permission is required for student use of a personal electronic device during classroom instruction or the classroom period.

11. Voice, video, and image capture applications may only be used with prior teacher permission and for specific instructional purpose(s).
12. The teacher may request at any time that the personal electronic device be turned off and put away. Failure to do so may result in disciplinary action and revocation of access to the network. See [Disciplinary Actions in this Responsible Use for Technology Resources Policy](#).
13. Sound should be muted unless the teacher grants permission for use of sound associated with the instructional activities.
14. The personal electronic device owner is the only person allowed to use the device.
15. No student shall use another student's district- or school-issued login credentials.
16. No student shall knowingly attempt to gain access to any computer, computer system, computer network, information storage media, or peripheral equipment without the consent of authorized school or district personnel.
17. No district-owned academic or productivity software can be installed on personal devices.
18. No student shall use any computer or device to illegally collect any electronic data or disrupt networking services. Students may not engage in any malicious use, disruption or harm to the school network, Internet services, learning environment or any other electronic device owned by the school, any school personnel and/or student.
19. Students may not attempt to use any software, utilities or other means to access Internet sites or content blocked by school district Internet filters.
20. Students may not use any personal electronic devices during any standardized assessments (RISE, Utah Aspire+, etc.) at any time.
21. Under the provisions of the Personal Electronic Device policy, parents who choose to allow students to use their own technology and students who bring personal technology do so knowing that it will diminish their expectation of privacy regarding their personal electronic device while at school.
22. The school reserves the right to search a personal electronic device in accordance with applicable laws and policies if there is reasonable suspicion that the student has violated: local, state, and/or federal laws, Kane School District policies, administrative procedures, school rules, or engaged in other misconduct while using the device.
23. Personal electronic devices are brought to school at the students' and parents' own risk. In the unlikely event that a personal device is lost, stolen or damaged, Kane School District is not responsible for any financial or data loss.
24. The school district and school district personnel is not responsible to repair, correct, or troubleshoot malfunctioning personal hardware or software.

Individual User Responsibilities

All users are expected to abide by the generally accepted rules of network etiquette (also known as netiquette). These rules include, but are not restricted to the following:

- a. **Be Polite and Use Appropriate Language** - Remember that you are a representative of your school and Kane School District on a non-private system. You may be alone using a technology resource or personal/Kane School District device, but what you say and do on your computer can be viewed globally. You should not submit, publish or display any defamatory, inaccurate, racially offensive, discriminatory,

abusive, obscene, profane, sexually oriented, harassing or threatening materials or messages either public or private.

- b. **Privacy** - Do not reveal any personal information about yourself or other persons (including, but not limited to, home address, personal phone numbers, photographs, or last name).

Users should have no expectation of privacy regarding their use of Kane School District property and technology resources. In general, communications or transmissions made through technology resources should never be considered private or confidential. Kane School District reserves the right to monitor the use of its network and all technology resources as it deems necessary to ensure the safety and integrity of its network, diagnose problems, investigate reports of illegal or impermissible activity and ensure user compliance with state and federal laws and Kane School District policies. In addition, users should be aware that Kane School District will comply with lawful orders of courts, such as subpoenas and search warrants.

Kane School District is subject to the [Utah Government Records Access and Management Act \(GRAMA\)](#) which may require disclosure of information transmitted through its technology resources, including email communications.

Kane School District is subject to the [Family Educational Rights and Privacy Act \(FERPA\)](#) which requires students educational records to be maintained in confidentiality. All Kane School District staff and employees will follow the guidelines of this law.

- c. **Electronic Mail (email)**

- a. All users of any electronic mail either provided by Kane School District or transmitted through Kane School District technology resources are required to comply with this Responsible Use Policy.
- b. System users are asked to purge email or outdated files on a regular basis. Employees and volunteers should ensure that any official school records that are maintained in an electronic medium that are subject to state or federal retention requirements are either retained in hard copy or archived prior to being deleted or purged.
- c. Never assume electronic mail is private. Messages relating to or in support of illegal activities must be reported to the authorities and Kane School District will comply with state and federal laws, as well as court orders or subpoenas that will require disclosure.
- d. Be brief and professional: Few people will bother to read a long message or one that is not narrowly tailored to the underlying purpose of the communication. Electronic communications by Kane School District employees, volunteers and staff should be consistent with Kane School District professional standards of conduct.
- e. Include your signature (name, position, affiliation, and Internet address) at the bottom of email messages.
- f. Send only to individuals and/or groups you know.

- d. **Disruptions** - Do not use the network in any way that would disrupt use of the network by others.

- e. **Ownership** - Any data or communication placed on Kane School District equipment will become the property of Kane School District. Intellectual property created solely for the purpose of satisfying a course requirement and/or contributing to their student learning is owned by the creator.

- f. **Vandalism** - Any attempt to alter or destroy data of another user will be subject to disciplinary or corrective action in accordance with Kane School District policy.

- g. **Accountability** - Users are responsible for the proper use of their system accounts, passwords and Kane School District-issued technology resources. Users must control unauthorized use of their accounts,

passwords and Kane School District-issued technology resources. Users should not provide their password to any person, unless authorized or directed by Kane School District. If you permit someone else access to your account, password, or Kane School District-issued technology resources, you may be held responsible for any improper, illegal or destructive activity done by that person. Do not give others access to Kane School District technology resources unless they are authorized and authenticated to do so. Users may not extend access to Kane School District technology resources to others without permission from Kane School District.

If you believe that your account, password or Kane School District-issued technology resource may have been stolen, hacked, or compromised, you must immediately report it to Kane School District's Technology Department. We also recommend In the event that a student believes that his/her password has been compromised, he/she should immediately reset his/her password.

EXCEPTIONS: If you are unable to follow any of these guidelines for any special circumstances, health related reasons or an emergency, prior approval is required from Kane School District.

Internet Safety

Kane School District makes the Internet accessible in accordance with our mission to provide information resources and services to ensure that all users have free and open access to ideas and information. In this role, Kane School District provides access to information resources available on the Internet. Kane School District has no control over the information obtained through the Internet and cannot be held responsible for its content or accuracy. It may contain materials which some find offensive or inappropriate. All staff, students and other users access the Internet at their own discretion.

In accordance with the federal [Children's Internet Protection Act \(CIPA\)](#), all desktop computers, laptops and personal/Kane School District wireless devices, that utilize Kane School District network, are being filtered by a centralized filtering appliance. This filtering appliance is set to screen out sites which may reasonably be construed as obscene, as that term is defined in section 1460 of title 18, United States Code; or child pornography, as that term is defined in section 2256 of title 18, United States Code; or harmful to minors as defined in section 1703, Pub. L. 106-544. Kane School District has the ability to monitor the online activities of students, staff and guests through direct observation and/or technological means to ensure that students, staff and guests are following the guidelines and policies set forth by Kane School District.

Kane School District Board Policy also prohibits harassment, bullying, retaliation, discrimination, and other conduct that creates a hostile working or educational environment for an individual. This prohibition extends to the use of Kane School District's technology resources. If you ever feel that you are being harassed, bullied, retaliated or discriminated against, or otherwise being subjected to illegal or inappropriate conduct through Kane School District's technology resources, you should immediately report it to Kane School District.

As with any other technology resource, restriction of a child's use of the Internet is ultimately the responsibility of the parent/legal guardian, within the confines of the law. See the [Parental Restriction on Use of Technology Resources section](#) below if parents do not wish for their students to use the technology resources of Kane School District.

Kane School District assumes no responsibility for damages, direct, or indirect, for the use of the Internet. This includes, but is not limited to, damage to Kane School District or personally owned devices caused by virus-laden material downloaded from any Internet site. Users are encouraged to purchase and use a virus detection program on their personal devices.

Users should be aware that the Internet is not a secure medium. It is possible for third parties to obtain information regarding an individual user's search activities. Users should be very cautious about providing personal information over the Internet.

Parental Restriction on Use of Technology Resources

Parents and/or Guardians who have objections to the Internet or other network-delivered services may assume responsibility for imposing restrictions only on their child(ren). Any parent wishing to restrict his/her child's access to such services must provide the school with this restriction in writing. For details, see Kane School District Board policy governing the selection and adoption of instructional materials.

Limitation of LEA Liability

Kane School District will not guarantee that the functions or services provided through Kane School District's network service will be without error. Kane School District will not be responsible for any damage you may suffer, including but not limited to loss of data, interruptions of service, or exposure to inappropriate material or people. Kane School District will not be responsible for the accuracy or quality of the information obtained through the system. Kane School District will not be responsible for financial obligations arising through the unauthorized use of the system. Your parents can be held financially responsible for any harm that may result from your intentional misuse of the system.

Definitions

Social Media - the interactive use of online resources including, but not limited to, Facebook, YouTube, Twitter, MySpace, Ning, Google Apps, Skype, chat rooms, wikis, and blogs.

Children's Internet Protection Act (CIPA) - The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-rate program – a program that makes certain communications technology more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA.

Personal Devices - the use of any technology related device that is not owned by Kane School District.

Digital Content - products available in digital form. It typically refers to music, information and images that are available for download or distribution on electronic media.

Hacking - to reconfigure or reprogram a [system](#) to function in ways not facilitated by the [owner](#), [administrator](#), or [designer](#).

Copyrighted - The legal right granted to an author, composer, playwright, publisher, or distributor to exclusive publication, production, sale, or distribution of a literary, musical, dramatic, or artistic work.

Computer Virus - a [computer program](#) that can copy itself and infect a computer. It is also being used as a catch-all phrase to include all types of [malware](#), [adware](#), and [spyware](#) programs that do not have the reproductive ability. Malware includes computer viruses, [worms](#), [trojans](#), most [rootkits](#), spyware, dishonest adware, [crimeware](#), and other malicious and unwanted software, including true viruses. Viruses are sometimes confused with [computer worms](#) and [Trojan Horses](#), which are technically different. A worm can exploit security vulnerabilities to spread itself automatically to other computers through networks, while a Trojan is a program that appears harmless but hides malicious functions. Worms and Trojans, like viruses, may harm a computer system's data or performance. Some

viruses and other malware have symptoms noticeable to the computer user, but many are surreptitious and go unnoticed.

Technology Resources - Any and all electronic devices, mass storage media, online display devices, computers, computer printouts, and all computer-related activities involving any device capable of receiving email, browsing Websites, receiving, storing, managing or transmitting data including but not limited to mainframes, servers, personal computers, notebook computers, laptops, smart phones, tablets, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, telecommunication devices, network environments, telephones, fax machines and printers. Technology resources also includes the procedures, equipment, facilities, software and data that is designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display and transmit information.

Guest - An individual: (a) who is not a student, employee, or designated volunteer of a public school; and (b) who is on school property or at the site of a school-sponsored activity or event.

Kane School District Student/Parent Policy Acknowledgement Form Responsible Use and Personal Electronic Devices Policies

Student Name _____ Student ID # _____

Responsible Use Policy - Parent and Student Agreement

I/we have read Kane School District [Responsible Use Policy](#) and understand and agree to the terms and conditions herein.

I/we understand that assignments and projects may be posted to teacher-approved blogs, Google Docs and other hosting sites. This may include personally identifiable information that may be classified as an educational record under FERPA (Family Education Records and Privacy Act).

I/we have signed and returned Kane School District Responsible Use Policy for the student indicated below.

I/we give permission for my student, (please print name) _____ to use school owned technology at _____ School.

Parent Signature _____ Date _____

I understand the above rules and policy for Responsible Use of Technology at _____ School and agree to follow the policies as outlined.

Student Signature _____ Date _____

Personal Electronic Device Policy Agreement

I/we have read and understand the Personal Electronic Device Policy and concerning the use and connection of privately owned electronic devices to Kane School District wireless network. This includes the use of a smartphone or other handheld device.

I/we understand that this policy form and the privilege to use privately owned electronic devices in school can be revoked at any time.

I/we understand that violation of these provisions may result in the confiscation of a personal electronic device by the school administration, any other designated school district representative, or local law enforcement and that legal action may occur.

I/we understand that we are responsible for compensating the school district for any losses, costs or damages incurred due to violations of **Kane School District** Board policies/procedures and school rules by the student in conjunction with the use of his/her personal electronic device, including the cost of investigating such violations.

1) Brand Name/Model:	
Serial Number:	
Virus Software Installed if applicable:	
2) Brand Name/Model:	
Serial Number:	
Virus Software Installed if applicable:	
3) Brand Name/Model:	
Serial Number:	

Virus Software Installed if applicable:	
---	--

I/we give permission for my student, (please print name) _____ to use a personal electronic device on the wireless network at _____ School.

Parent Signature _____ Date _____

I understand the above rules and policy for connecting a personal electronic device to the wireless network at _____ School and agree to follow the rules outlined.

Student Signature _____ Date _____

G Suite for Education to Parents and Guardians

To parents and guardians,

At Kane School District, we use G Suite for Education, and we are seeking your permission to provide and manage a G Suite for Education account for your child. G Suite for Education is a set of education productivity tools from Google including Gmail, Calendar, Docs, Classroom, and more used by tens of millions of students and teachers around the world. At Kane School District, students will use their G Suite accounts to complete assignments, communicate with their teachers, [if applicable, insert sign into their Chromebooks], and learn 21st century digital citizenship skills.

The notice below provides answers to common questions about what Google can and can't do with your child's personal information, including:

- What personal information does Google collect?
- How does Google use this information?
- Will Google disclose my child's personal information?
- Does Google use student personal information for users in K-12 schools to target advertising?
- Can my child share information with others using the G Suite for Education account?

Please read it carefully, let us know of any questions, and then sign below to indicate that you've read the notice and give your consent. If you don't provide your consent, we will not create a G Suite for Education account for your child. However, if you refuse to sign this agreement, this will negatively impact the ability for your student to complete coursework as many assignments are completed use G Suite apps and students need a G Suite account to sign into and use a chromebook.

I give permission for [insert name of school/district] to create/maintain a G Suite for Education account for my child and for Google to collect, use, and disclose information about my child only for the purposes described in the notice below.

Thank you,

[Insert name of school administrator]

Full name of student

Printed name of parent/guardian

Signature of parent/guardian

Date

G Suite for Education Notice to Parents and Guardians

This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from students in connection with these accounts.

Using their G Suite for Education accounts, students may access and use the following “Core Services” offered by Google (described at https://gsuite.google.com/terms/user_features.html):

- Gmail
- Google+
- Calendar
- Chrome Sync
- Classroom
- Cloud Search
- Contacts
- Docs, Sheets, Slides, Forms
- Drive
- Groups
- Hangouts, Hangouts Chat, Hangouts Meet, Google Talk
- Jamboard
- Keep
- Sites
- Vault

Google provides information about the information it collects, as well as how it uses and discloses the information it collects from G Suite for Education accounts in its G Suite for Education Privacy Notice. You can read that notice online at https://gsuite.google.com/terms/education_privacy.html You should review this information in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a student account, Kane School District may provide Google with certain personal information about the student, including, for example, a name, email address, and password. Google may also collect personal information directly from students, such as telephone number for account recovery or a profile photo added to the G Suite for Education account.

When a student uses Google services, Google also collects information based on the use of those services. This includes:

- device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number;
- log information, including details of how a user used Google services, device event information, and the user's Internet protocol (IP) address;
- location information, as determined by various technologies including IP address, GPS, and other sensors;
- unique application numbers, such as application version number; and
- cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

How does Google use this information?

In G Suite for Education Core Services, Google uses student personal information to provide, maintain, and protect the services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.

Does Google use student personal information for users in K-12 schools to target advertising?

No. For G Suite for Education users in primary and secondary (K-12) schools, Google does not use any user personal information (or any information associated with an G Suite for Education Account) to target ads, whether in Core Services or in other Additional Services accessed while using an G Suite for Education account.

Can my child share information with others using the G Suite for Education account?

We may allow students to access Google services such as Google Docs and Sites, which include features where users can share information with others or publicly. When users share information publicly, it may be indexable by search engines, including Google.

Will Google disclose my child's personal information?

Google will not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

- With parental or guardian consent. Google will share personal information with companies, organizations or individuals outside of Google when it has parents' consent (for users below the age of consent), which may be obtained through G Suite for Education schools.
- G Suite for Education accounts, because they are school-managed accounts, give administrators access to information stored in them.
- For external processing. Google may provide personal information to affiliates or other trusted businesses or persons to process it for Google, based on Google's instructions and in compliance with the G Suite for Education privacy notice and any other appropriate confidentiality and security measures.
- For legal reasons. Google will share personal information with companies, organizations or individuals outside of Google if it has a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:
 - meet any applicable law, regulation, legal process or enforceable governmental request.
 - enforce applicable Terms of Service, including investigation of potential violations.
 - detect, prevent, or otherwise address fraud, security or technical issues.
 - protect against harm to the rights, property or safety of Google, Google users or the public as required or permitted by law.

Google also shares non-personal information -- such as trends about the use of its services -- publicly and with its partners.

What choices do I have as a parent or guardian?

First, you can consent to the collection and use of your child's information by Google. If you don't provide your consent, we will not create a G Suite for Education account for your child, and Google will not collect or use your

child's information as described in this notice.

If you consent to your child's use of G Suite for Education, you can access or request deletion of your child's G Suite for Education account by contacting [insert contact information for school administrator]. If you wish to stop any further collection or use of your child's information, you can request that we use the service controls available to limit your child's access to features or services, or delete your child's account entirely. You and your child can also visit <https://myaccount.google.com> while signed in to the G Suite for Education account to view and manage the personal information and settings of the account.

What if I have more questions or would like to read further?

If you have questions about our use of Google's G Suite for Education accounts or the choices available to you, please contact Travis Terry, IT Director Kane School District, terryt@kanek12.org. If you want to learn more about how Google collects, uses, and discloses personal information to provide services to us, please review the [G Suite for Education Privacy Center](https://www.google.com/edu/trust/) (at <https://www.google.com/edu/trust/>), the [G Suite for Education Privacy Notice](https://gsuite.google.com/terms/education_privacy.html) (at https://gsuite.google.com/terms/education_privacy.html), and the [Google Privacy Policy](https://www.google.com/intl/en/policies/privacy/) (at <https://www.google.com/intl/en/policies/privacy/>).

The Core G Suite for Education services are provided to us under [Google's Apps for Education agreement](https://www.google.com/apps/intl/en/terms/education_terms.html) (at https://www.google.com/apps/intl/en/terms/education_terms.html) [if school/district has accepted the Data Processing Amendment (see <https://support.google.com/a/answer/2888485?hl=en>), insert: and the [Data Processing Amendment](https://www.google.com/intl/en/work/apps/terms/dpa_terms.html) (at https://www.google.com/intl/en/work/apps/terms/dpa_terms.html)].