



Beavercreek City Schools (BCS), is providing students with a mobile device for use during and after school hours. This device is the property of BCS and should be treated as an educational tool similar to a course textbook. Currently, Grades K-2 will receive an iPad, and grades 3-12 will receive a Chromebook.

Mobile devices provide access to many educational materials needed for classroom studies including Google Apps for Education, online textbooks and district provided web-based resources. Students will use their mobile device regularly in their classes to complete homework and school projects. The supplied device is an educational tool and not intended for gaming, social networking, or high end computing.

The policies, procedures and information within this document apply to all mobile devices used at Beavercreek City Schools by students, staff or guests and includes any other device considered by the Administration to fall under this policy.

Teachers may set additional requirements for mobile device use in their classroom.

Receiving Your mobile device:

Parents & students must complete the Mobile Device Agreement portion of the OneView online forms prior to being allowed to take the mobile device home.

Mobile Device Care Plan:

Beavercreek City Schools has an optional Mobile Device Care Plan. The annual cost is \$20 per device. Joining the program provided reduced cost for repairs or replacement of mobile devices. Look for the Mobile Device Care Program document in the addendum for more information.

Pickup:

Once the online agreement is completed, the student will be provided with the following:

- A mobile device (iPad K-2, Chromebook 3-12)
- A charging block/cord
- A device case

Each building determines the process they use to handout the devices.

Optional Accessories:

The following items are not provided by BCS but may be helpful when working on a mobile devices:

- Headphones/ 'ear-buds' (with built in microphone, if desired)
- Stylus
- Flash drive (Chromebook only)

Training:

Students will be trained on how to use the mobile device and access commonly used web-based applications available to them. Training documents and videos will be available online for students to refer to as needed.

Return:

Students will retain their original mobile device each year while enrolled at BCS. Any student who transfers out of BCS will be required to return their mobile device and accessories.

If a mobile device and/or accessories are not returned, outstanding fees will be added to the student's account. Unpaid fees can result in the withholding of transcripts or other transfer information.

The cost of replacement for a mobile device or any of its accessories that are lost or intentionally damaged is the responsibility of the student and parent involved in the loss or damage of property. The costs will change based on current replacement cost - the family will be charged the amount the district pays for the replacement parts.

Taking Care of Your Mobile Device:

Students are responsible for the general care of the mobile device issued to them by BCS. Mobile Devices that are broken or fail to work properly must be taken to the area designated in each building for repair. If a loaner mobile device is needed, one will be issued to the student until their designated device can be repaired or replaced.

Each device will be pre-labeled in the manner specified by BCS. This includes individual student identification and a device asset tag. Under no circumstances are students to modify, remove, or destroy identification labels.

General Precautions:

- Devices must be kept in their protective cases at all times. Damage incurred to a device not in its case will be charged at the full rate of repair.
- Food and open drink containers should be kept a reasonable distance from a device while it is in use.
- Cords, cables, and removable storage devices should be carefully inserted and removed from the device.
- Students should never carry their device while the screen is open unless directed to do so by a teacher.
- Devices should be shut down when not in use to conserve battery life.
- Devices should never be handled roughly. This includes such treatment as shoving it into a locker or wedging it into a book bag.
- Do not expose your device to extreme temperatures or direct sunlight for extended periods of time as these may cause damage to the device.
- Do not store your device outside or in a vehicle (especially overnight).

- Allow your device to reach room temperature prior to turning it on.
- Do not place anything on the device before closing the lid (e.g. pens, pencils, notebooks).
- Do not lean on, bend, poke or apply pressure to the device. The protective case is not meant to withstand strong pressure.
- Clean the screen with a soft, dry anti-static, or micro-fiber cloth. Do not use window cleaner or any type of liquid or water on the mobile device screen.

Personalizing the Mobile Device:

BCS considers mobile devices an educational tool similar to a course textbook. As such, devices must remain free of any writing, drawing or stickers. An identification label with the student's name is acceptable to place on a device and/or case. Spot checks for compliance may be done by an administrator or BCS technician at any time.

Students may add appropriate music, photos, and videos to their device.

Personalized media are subject to inspection and must follow the BCS acceptable use policy. A student may be asked to restart their mobile device at any time, clearing the device of temporary files.

Using Your Mobile Device at School:

The device is intended for use at school each day. Students are expected to bring their mobile device to all classes unless specifically advised not to do so by their teacher. In addition to teacher expectations for device use, resources such as school messages, announcements, calendars, student handbooks and schedules will be accessed using the device. Mobile devices will be used for district and state testing.

Students do not need to carry the AC Adapter power cord (charger) to school. Limited charging will be available during the school day.

Sound:

It is highly recommended that a student bring personal headphones or 'ear-buds' for any audio/video files they wish to access. A built in microphone feature may also be helpful for some projects.

Printing:

Google's Cloud Print service is used by BCS to provide printing options to students. Printers is not available everywhere. District and building administration will work together to make sure printing needs are covered.

Storing Your Mobile Device:

When students are not using their mobile device, **they should be securely stored**. Nothing should be placed on top of the device when it is being stored.

Storing Mobile Devices at Extracurricular Events:

Students are responsible for securely storing their devices during extra-curricular or after school events. Mobile devices should never be left in unattended book bags or backpacks. Do not ask another student to look after your device.

Unsupervised Mobile Devices

Mobile devices found in unsupervised areas will be confiscated by staff and taken to the main office. Disciplinary action may be taken for leaving a device in an unsupervised location

Using Your Mobile Device at Home:

Mobile devices are to be taken home each night for charging. ***Devices must be brought to school each day fully charged.*** A fully charged device should last the duration of a normal school day.

When using home Wi-Fi networks, the device will continue to utilize school proxy servers. Web search results will be filtered by district web filtering tools.

Printing:

The devices will not support a physical printer connection. Google's Cloud Print service may allow Chromebooks to print to a home printer through a wireless home network.

Additional Cloud Print resources are available at <http://google.com/cloudprint>

Managing and Saving Files:

Every BCS student will be provided by the district with an individual Google Education account. Students are responsible for saving documents to their Google Drive. They may also use an external memory device such as an SD card or USB flash drive to save their files. Google accounts are accessible through any internet connection and

allow sharing and collaboration with teachers and students. It is the responsibility of the student to maintain the integrity of their files and keep proper backups.

Software and Apps:

Chromebook software is delivered via the Chrome Web Store and managed by the BCS Technology Department. Other than its operating system (OS) and security features, the device only utilizes web-based applications (apps) that do not require installation space on a hard drive. Some applications allow for offline use. These create temporary files on a Chromebook so long as it remains logged in to a single user's account. The software apps originally installed on the Chromebook must remain on the device in usable condition and easily accessible at all times.

All Chromebooks are supplied with the latest build of Google Chrome OS. Software updates are installed automatically when the machine is restarted. Shutting down and restarting should be performed on a regular basis.

From time to time BCS may add software applications for use in a particular course or for a specific purpose (such as district and state testing). This process will be automatic with limited impact on students. Applications that are no longer needed will automatically be removed by the school whenever possible.

Non-District Software:

Students are not permitted to install additional software on their mobile device beyond what has been approved by Beaver Creek City Schools.

Inspection:

Students may be selected at random to provide their mobile device for inspection. The purpose for inspection will be to check for proper care and maintenance as well as inappropriate materials being carried into the school.

Repairing or Replacing Your Mobile Device:

Basic Troubleshooting:

If technical difficulties occur with a device, the easiest method of attempting to resolve the problem is to shutdown and restart the device. This will clear any temporary files and update the OS software.

If the issue remains unresolved, take the device to the designated area of the building to obtain technical support.

Under no circumstances should a student, parent or other individual attempt to self-repair or otherwise obtain their own repairs for a damaged or non-functioning mobile device.

Mobile Devices Undergoing Repair:

- Building technicians may choose to restore the device to factory defaults. This will restore the device to the state in which it was originally received. Any temporary files on the device will be erased. Files stored on external media (SD card or USB flash drive), or in a Google account are not stored locally and will be intact after the operating system is restored.
- A loaner device will be provided to a student if their device cannot be quickly repaired.

BCS reserves the right to charge to the student's account the full cost of repairs for mobile device damage that is the result of misuse or abusive handling. Insurance will not cover damage of this type to a device.

Addendum 1 - Mobile Device Care Program

Students and parents are responsible for district-owned technology property issued to them, just as they are for other district-owned items such as textbooks, athletic equipment and library books. The district will repair or replace the devices, but the students and parents are responsible for the cost of those repairs or replacements that occur due to misuse, abuse or negligence. Defective and normal wear issues will not be charged to families. For example, a dead battery in a mobile device will be fixed without charging families. Replacement costs (lost/stolen) are not covered by the program.

To help offset the liability of the families, Beavercreek City Schools is offering a Mobile Device Care Program. For \$20 per year, per device, the Mobile Device Care Program will repair or replace the device at a significant savings to the family. Enrolling in the program is optional. The table below show the price structure for repairs and replacements with the plan and without the plan.

Repair costs - charged per device each repair

All repairs are charged at the level in the chart or at the cost of the repair - whichever is less

	1st repair	2nd repair	3rd or greater repair
Without Mobile Device Care Program	Repair Cost	Repair Cost	Repair Cost
With Mobile Device Care Program	\$0	\$25	\$50

Example scenario 1: a student breaks the screen on an iPad twice in a year. *The current cost to the district to replace a screen is \$115 per instance.*

Without Mobile Device Care Program	\$115	1st repair
	\$115	2nd repair
	\$230	Total
With Mobile Device Care Program	\$20	Program cost
	\$0	1st repair
	\$25	2nd repair
	\$45	Total

Example scenario 2: a student breaks the screen on an iPad three times in a year. *The current cost to the district to replace screen is \$115.*

Without Mobile Device Care Program	\$115	1st repair
	\$115	2nd repair
	\$115	3rd repair
	\$345	Total
With Mobile Device Care Program	\$20	Program cost
	\$0	1st repair
	\$25	2nd repair
	\$50	3rd repair
	\$95	Total

Addendum 2 - AUP

Beavercreek City Schools

STUDENT EDUCATION TECHNOLOGY ACCEPTABLE USE AND SAFETY

Administrative Guideline

Students shall use District Technology Resources (see definition Bylaw 0100) for educational purposes only. District Technology Resources shall not be used for personal, non-school related purposes. Use of District Technology Resources is a privilege, not a right. When using District Technology Resources, students must conduct themselves in a responsible, efficient, ethical, and legal manner. Students found to have engaged in unauthorized or inappropriate use of District Technology Resources, including any violation of these guidelines, may have their privilege limited or revoked, and may face further disciplinary action consistent with the Student Handbook, and/or civil or criminal liability. Prior to accessing or using District Technology Resources, students and parents of minor students must sign the Student Technology Acceptable Use and Safety Agreement (Form 7540.03 F1). Parents should discuss their values with their children and encourage students to make decisions regarding their use of District Technology Resources that is in accord with their personal and family values, in addition to the Board's standards.

This guideline also governs students' use of their personal communication devices (see definition Bylaw 0100) when they are connected to District Technology Resources, or when used while the student is on Board-owned property or at a Board-sponsored activity.

Below is a non-exhaustive list of unauthorized uses and prohibited behaviors. This guideline further provides a general overview of the responsibilities users assume when using District Technology Resources.

- A. All use of District Technology Resources must be consistent with the educational mission and goals of the District.
- B. Students may only access and use District Technology Resources by using their assigned account and may only send school-related electronic communications using their District-assigned e-mail addresses. Use of another person's account/e-mail address is prohibited. Students may not allow other users to utilize their account/e-mail address and should not share their password with other users. Students may not go beyond their authorized access. Students should take steps to prevent unauthorized access to their accounts by logging off or "locking" their computers/laptops/tablets/personal communication devices when leaving them unattended.
- C. No user may have access to another's private files. Any attempt by users to access another user's or the District's non-public files, or phone or e-mail messages is considered theft. Any attempts to gain access to unauthorized resources or information either on the District's computer or telephone systems or any systems to which the District has access are prohibited. Similarly, students may not intentionally seek information on, obtain copies of, or modify files, data or passwords belonging to other users, or misrepresent other users on the District's Network.
- D. Students may not intentionally disable any security features used on District Technology Resources.
- E. Students may not use District Technology Resources or their personal communication devices to engage in vandalism, "hacking," or other illegal activities (e.g., software pirating;

intellectual property violations; engaging in slander, libel, or harassment; threatening the life or safety of another; stalking; transmission of obscene materials or child pornography, including sexting; fraud; sale of illegal substances and goods).

1. Slander and libel - In short, slander is "oral communication of false statements injurious to a person's reputation," and libel is "a false publication in writing, printing, or typewriting or in signs or pictures that maliciously damages a person's reputation or the act or an instance of presenting such a statement to the public." (The American Heritage Dictionary of the English Language. Third Edition is licensed from Houghton Mifflin Company. Copyright © 1992 by Houghton Mifflin Company. All rights reserved.) Students shall not knowingly or recklessly post false or defamatory information about a person or organization. Students are reminded that material distributed over the Internet is "public" to a degree no other school publication or utterance is. As such, any remark may be seen by literally millions of people and harmful and false statements will be viewed in that light.
2. Students shall not use District Technology Resources to transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex, sexual orientation or transgender identity, age, disability, religion, or political beliefs. 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 is grounds for discipline. Such actions will be reported to local law enforcement and child services as required by law.
3. Vandalism and Hacking – Deliberate attempts to damage the hardware, software, or information residing in District Technology Resources or any computer system attached through the Internet is strictly prohibited. In particular, malicious use of District Technology Resources to develop programs that harass other users or infiltrate a computer/laptop/tablet or computer system and/or damage the software components of a computer or computing system is prohibited.

Attempts to violate the integrity of private accounts, files or programs, the deliberate infecting of the network or computers, laptops, tablets, etc., attached to the network with a "virus", attempts at hacking into any internal or external computer systems using any method will not be tolerated.

Students may not engage in vandalism or use District Technology Resources or their personal communication devices in such a way that would disrupt others' use of District Technology Resources.

Vandalism is defined as any malicious or intentional attempt to harm, steal, or destroy data of another user, school networks, or technology hardware. This includes but is not limited to uploading or creation of computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass network security and/or the Board's technology protection measures. Students also must avoid intentionally wasting limited resources. Students must immediately notify the teacher, building Principal, or IT Staff if they identify a possible security problem. Students should not go looking for security problems, because this may be construed as an unlawful attempt to gain access.

Students shall not use District Technology Resources to access, process, distribute, display or print prohibited material at any time, for any

purpose. Students may only access, process, distribute, display or print restricted material, and/or limited access material as authorized below.

- a. Prohibited material includes material that constitutes child pornography and material that is obscene, objectionable, inappropriate and/or harmful to minors, as defined by the Children's Internet Protection Act. As such, the following material is prohibited: material that appeals to a prurient or unhealthy interest in nudity, sex, and excretion; material that 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 material that lacks serious literary, artistic, political or scientific value as to minors. Prohibited material also includes material that appeals to a prurient or unhealthy interest in, or depicts, describes, or represents in a patently offensive way, violence, death, or bodily functions; material designated as for "adults" only; and material that promotes or advocates illegal activities.
- b. Restricted material may not be accessed by elementary or middle school students at any time, for any purpose. Restricted material may be accessed by high school students in the context of specific learning activities that have been approved by a teacher or staff member for legitimate research purposes. Materials that may arguably fall within the description provided for prohibited material that have clear educational relevance, such as material with literary, artistic, political, or scientific value, will be considered to be restricted. In addition, restricted material includes materials that promote or advocate the use of alcohol and tobacco, hate and discrimination, satanic and cult group membership, school cheating, and weapons. Sites that contain personal advertisements or facilitate making online connections with other people are restricted unless such sites have been specifically approved by the Administrators.
- c. Limited access material is material that is generally considered to be non-educational or entertainment. Limited access material may be accessed in the context of specific learning activities that are directed by a teacher or during periods that a school may designate as "open access" time. Limited access material includes such material as electronic commerce, games, jokes, recreation, entertainment, sports, and investment.

If a student inadvertently accesses material that is considered prohibited or restricted, s/he should immediately disclose the inadvertent access to the teacher or building Principal. This will protect the student against an allegation that s/he intentionally violated the provision.

The determination of whether material is prohibited, restricted, or limited access shall be based on the content of the material and the intended use of the material, not on the protective actions of the technology protection measures. The fact that the technology protection measures have not protected against access to certain material shall not create the presumption that such material is appropriate for students to access. The fact that the technology protection measures have blocked access to certain material shall not create the presumption that the material is inappropriate for students to access.

4. Unauthorized Use of Software or Other Intellectual Property from Any Source – All communications and information accessible via the Internet should be assumed to be

private property (i.e., copyrighted and/or trademarked). Laws and ethics require proper handling of intellectual property. All copyright issues regarding software, information, and attributions/acknowledgement of authorship must be respected.

Software is intellectual property, and, with the exception of freeware, is illegal to use without legitimate license or permission from its creator or licensor. All software loaded on District computers must be approved by the Technology Director, and the District must own, maintain, and retain the licenses for all copyrighted software loaded on District computers. Students are prohibited from using District Technology Resources for the purpose of illegally copying another person's software. Illegal peer-to-peer file trafficking of copyrighted works is prohibited.

Online articles, blog posts, podcasts, videos, and wiki entries are also intellectual property. Students should treat information found electronically in the same way they treat information found in printed sources – i.e., properly citing sources of information and refraining from plagiarism. Rules against plagiarism will be enforced.

- F. Transmission of any material in violation of any State or Federal law or regulation, or Board policy is prohibited.
- G. District Technology Resources may not be used for private gain or commercial purposes (e.g., purchasing or offering for sale personal products or services by students), advertising, or political lobbying. This provision shall not limit the use of District Technology Resources for the purpose of communicating with elected representatives or expressing views on political issues.
- H. Use of District Technology Resources to engage in cyberbullying is prohibited. "Cyberbullying" involves the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, which is intended to harm others. [Bill Belsey (<http://www.cyberbullying.org>)] Cyberbullying may occur through e-mail, instant messaging (IM), chat room/Bash Boards, small text-messages (SMS), websites, voting booths.

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 negatively impact the victim's use of that method of communication and/or 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.
- I. Students are expected to abide by the following generally-accepted rules of online etiquette:
 - 1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through or utilizing District Technology Resources Do not use obscene, profane, lewd, vulgar, rude, inflammatory, sexually explicit, defamatory, threatening, abusive or disrespectful language in communications made through or utilizing District Technology

Resources.

2. Do not engage in personal attacks, including prejudicial or discriminatory attacks.
 3. Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending him/her messages, the student must stop.
 4. Do not post information that, if acted upon, could cause damage or a danger of disruption.
 5. 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 Internet. This prohibition includes, but is not limited to, disclosing personal identification information on commercial websites.
 6. Do not transmit pictures or other information that could be used to establish your identity without prior approval of a teacher.
 7. Never agree to get together with someone you "meet" on-line without parent approval and participation.
 8. Check e-mail frequently, and delete e-mail promptly.
 9. Students should promptly disclose to a teacher or administrator any messages they receive that are inappropriate or make 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 an administrator.
- J. Downloading of files onto school-owned equipment or contracted online educational services is prohibited, without prior approval from Department of Technology. If a student transfers files from information services and electronic bulletin board services, the student must check the file with a virus-detection program before opening the file for use. Only public domain software may be downloaded. If a student transfers a file or installs a software program that infects District Technology Resources with a virus and causes damage, the student will be liable for any and all repair costs to make the District Technology Resources once again fully operational.
- K. Students must secure prior approval from a teacher or the Department of Technology before joining a Listserv (electronic mailing lists) and should not post personal messages on bulletin boards or Listservs.
- L. Students may use real-time electronic communication, such as chat or instant messaging, only under the direct supervision of a teacher or in moderated environments that have been established to support educational activities and have been approved by the Board, Superintendent, or building principal. Students may only use their school-assigned accounts/email addresses when accessing, using or participating in real-time electronic communications for education purposes.

Users have no right or expectation to privacy when using the District Technology Resources. The Board reserves the right to access and inspect any facet of its Technology Resources, including, but not limited to, computers, laptops, tablets, and other web-enabled devices, networks, or Internet connections or online educational services or apps, 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 District Technology Resources 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 Technology Resources and related storage medium and equipment. Routine maintenance and monitoring, utilizing both technology 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 have the right to request to see the contents of their children's files, e-mails and records.

- M. Use of the Internet and any information procured from the Internet is at the student's own risk. The Board makes no warranties of any kind, either express or implied, that the functions or the services provided by or through District Technology Resources will be error-free or without defect. The Board is not responsible for any damage a user may suffer, including, but not limited to, loss of data, service interruptions, or exposure to inappropriate material or people. The Board is not responsible for the accuracy or quality of information obtained through the Internet. Information (including text, graphics, audio, video, etc.) from Internet sources used in student papers, reports, and projects must be cited the same as references to printed materials. The Board is not to be responsible for financial obligations arising through the unauthorized use of its Technology Resources. Students or parents of students will indemnify and hold the Board harmless from any losses sustained as the result of a student's misuse of District Technology Resources.
- N. Disclosure, use and/or dissemination of personally identifiable information of minors via the Internet is prohibited, except as expressly authorized by the minor student's parent/guardian on the "Student Technology Acceptable Use and Safety Agreement Form."
- O. Proprietary rights in the design of websites hosted on Board-owned or leased servers remains at all times with the Board.
- P. File-sharing is strictly prohibited. Students are prohibited from downloading and/or installing file-sharing software or programs on District Technology Resources.
- Q. Students may not use District Technology Resources to establish or access web-based e-mail accounts on commercial services (e.g., Gmail, iCloud, Outlook, Yahoo mail, etc.).
- R. Since there is no central authority on the Internet, each site is responsible for its own users. Complaints received from other sites regarding any of the District's users will be fully investigated and disciplinary action will be taken as appropriate.
- S. Game playing is not permitted unless under the supervision of a teacher.

Abuse of Network Resources

Peer-to-peer file sharing, mass mailings, downloading of unauthorized games, videos, and music are wasteful of limited network resources and are forbidden. In addition, the acquisition and sharing of copyrighted materials is illegal and unethical.

Unauthorized Printing

District printers may only be used to print school-related documents and assignments. Printers, like other school resources, are to be used in a responsible manner. Ink cartridges and paper, along with printer repairs and replacement are very expensive. The District monitors printing by user. Print jobs deemed excessive and abusive of this privilege may result in charges being

assessed to the student. Users are prohibited from replacing ink cartridges and performing any other service or repairs to printers. Users should ask, as appropriate, for assistance to clear paper that is jamming a printer.

Monitoring

The District utilizes a technology monitoring system that conducts keyword searches of District Technology Resources supplied to students. These searches are conducted on district-issued student devices and accounts. These automated searches are conducted regardless of where the device is located, including school grounds, home or other location when using district technology or accounts. These automated searches may be conducted regardless of the time of day, including during school hours, after hours, weekend and holidays.

Once concerns are identified, a notification or “alert” will be sent to school district personnel, which may include: the Department of Technology, the Director of Pupil Services, Counselor, Principal, Assistant Principal, Safety and Security Officer, Superintendent of Schools and Assistant Superintendents. Designated personnel will review and evaluate the alert for content and credibility. In the event an emergency response is warranted, parents and/or local police authorities may be contacted.

The District cannot and does not assume any duty or obligation to continuously monitor any notifications or alerts, but will use the monitoring software as an aid to monitor district technology and accounts. While school staff will make reasonable efforts to supervise and monitor the use of technology, it is impossible to supervise at all times. The District has taken available precautions to restrict access to controversial materials. However, on a global network, it is impossible to control all materials and users may discover controversial information. In addition, the alerts and monitoring can serve as an aid in the prevention or detection of potential self-harm or cyberbullying, but are no guarantee.

Any questions and concerns regarding these guidelines may be directed to Department of Technology.