Carlisle Area School District
Guidelines for Acceptable Use of Technologies (Board Policy #815)
Revised July, 2022

Students, Teachers, Staff, Volunteers, Student Teachers, Consultants, Presenters, and Guests

I. Purpose

Access to various forms of technology, including the internet, computers, and other networked technology, are to facilitate learning, teaching, and daily operations through interpersonal communications and access to information, research, and collaboration. The district has developed carefully considered guidelines to ensure that district resources are not misused and that the computer systems are used only for legitimate and authorized purposes. These guidelines are supported through Board Policy 815 which can be viewed at www.carlisleschools.org/AUPPolicy815.

The district provides students, staff and other authorized individuals with access to district-owned devices, electronic communication systems, and the district network, which includes Internet access. With the Internet also comes the availability of material that may not be of value in the context of the school setting. The district firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the district.

II. Definition

District technology includes all computers (desktops and laptops), tablets (iPads), peripherals, software, data storage devices, local and wide area network devices, the Internet to include all on-line applications to which the school network may be linked, all data stored on district technologies, and all other networked resources.

III. Authority

The availability of access to electronic information does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.

The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, receive or display on or over the district's Internet, computers or network resources, including personal files or any use of the district's Internet, computers or network resources whether on or off district property. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The district shall cooperate to the extent legally required with the internet service provider, local, state, and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers, and network resources.

The district reserves the right to confiscate technologies that may be used in a malicious manner on the district network.

The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through the use of software and/or online server blocking. Specifically, the district operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. However, on a global network, it is impossible to control all materials and an industrious user may discover controversial information. The technology protection measure shall be enforced during use of computers with Internet access.

IV. Guidelines for Acceptable Use

Any or all use of the technologies defined are intended for authorized business and/or educational activities by students, parents, faculty, and community. The technologies are not intended for personal use.

Students, staff and other authorized individuals have the responsibility to respect and protect the rights of every other user in the district and on the Internet.

Network accounts shall be used only by the authorized owner of the account for its approved purpose. Network users shall respect the privacy of other users on the system.

Any user who determines that there may be a misuse of the technology within the organization, receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher, principal, supervisor, or the Technology Director immediately.

> High School Information for CTE Technology Classes Only: Students may be required to download software to their network directory for use on computers in these course classrooms. Students in these courses may be instructed to configure operating systems, move hardware, and install software as part of the specific course curriculum. These activities may only occur as indicated by the course instructor during class time on classroom computers that are not connected to the district network.

Prohibitions

Users are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Facilitating illegal activity.
2. Commercial or for-profit purposes.
3. Non-work or non-school related work.
4. Product advertisement or political lobbying.
5. Bullying/Cyberbullying.
6. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
8. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.
9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
10. Inappropriate language or profanity.
11. Transmission of material likely to be offensive or objectionable to recipients.
12. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
13. Impersonation of another user, anonymity, and pseudonyms.
14. Fraudulent copying, communications, or modification of materials in violation of copyright laws.
15. Loading or using of unauthorized games, programs, files, or other electronic media.
16. Disruption of the work of other users.
17. Destruction, modification, abuse or unauthorized access to network hardware, software and files.
18. Accessing the Internet, district computers or other network resources without authorization.
19. Disabling or bypassing the Internet blocking/filtering software without authorization.
20. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.
21. Any action, on or off campus, that causes, or is reasonably foreseeable to cause substantial disruption to the school environment.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, these guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.
2. Users are not to use a computer that has been logged in under another user's name.
3. Any user identified as a security risk or having a history of problems with other computers systems may be denied access to the network.

All employees, students, and approved volunteers have obligations under federal law to protect students' personally identifiable information and certain personal employee information from any unauthorized access, disclosure or release. Employees, students, and approved volunteers must comply with all applicable laws and should exercise caution, and utilize appropriate security measures such as password protection on their electronic devices, to prevent any unauthorized access to sensitive data. In no case shall employees store sensitive data locally on the hard drive or internal memory of the employee's personal electronic device. Sensitive data may only be stored in resources issued by and/or controlled by the district. Sensitive data must never be stored on personal devices or peripherals.

Software/Applications

All software is to be used in accordance with its license agreement. Software copyright infringement is illegal. The law surrounding copyright infringement affects not only the offending individual but also the district. Any questions or concerns regarding the legality of software should be referred to the Technology Director.

All software used by the district on district-owned computers will be purchased through the technology department. All software is to be delivered to the technology department for completion of registration and inventory requirements. Software must be registered in the name of the Carlisle Area School District and will include the job title or department in which it will be used.

All software will be authorized and installed by the technology department. The technology department may approve other users to install a specific software program on a specific computer(s). Once software is installed, the original media will be kept in a storage area maintained by the technology department.

A list of approved applications installed on tablets (iPads) devices can be found at www.carlisleschools.org/apps.

Users will not distribute software to any outsiders including consultants, trainers, student teachers, or any personal contacts.

No unauthorized software, shareware, freeware, web service, portable application, or other executable file may be downloaded, copied, used, or saved to any district-owned technology device, without prior permission of the Technology Director.

Hardware and Peripheral Technologies

Personal devices (including cell phones, printers, laptops, etc.) are to be utilized at the owner's risk. It is not the responsibility of the district to repair or replace the device in cases where the device is damaged, lost, stolen, does not function properly or is incompatible. The district reserves the right to disconnect personal devices or disable services without notification.

Personal *network* equipment is prohibited to be used onsite without receiving permission from the Director of Technology. Additionally, no personal device is permitted to be hard wired (*connected using Ethernet Cable*) to the CASD network.

No equipment shall be moved between classrooms, offices, and buildings or discarded without prior permission of the Director of IT Operations.

All users must make reasonable efforts to protect against theft or damage of district equipment. Technology devices left unattended must be secured.

No alterations, upgrades, or modifications may be made to hardware unless approved by the Director of IT Operations.

Personal media such as data disks, CDs, DVDs, and USB devices may be used to transfer files that are directly related to classroom assignment or administrative function. Any other file transfer between the district network and personal media is strictly prohibited.

All district technology supplies, including paper, ink and media are to be used for educational, administrative, and business purposes only.

The district is not liable or responsible for the loss of or damage to any electronic device that an employee or student brings to school, extra-curricular activities, or to school sponsored events or trips.

Network, Including Internet and Email Use
Network accounts are created by the technology department and are the property of the Carlisle Area School District. Students and staff are responsible to maintain a confidential password to their account.

Staff must change their password no less then every six months using the password guidelines posted on the district shared drive.

Users may not share their network or application account passwords with anyone. This applies to all programs, databases, and web-based systems including but not limited to district and teacher websites, PowerSchool, PowerTeacher, Schoology, Seesaw, USA Test Prep, 4Sight, GRADE, Dibels, and all Pennsylvania Department of Education applications. Student teachers and day to day substitutes should use the PowerTeacher Substitute logon to take attendance in PowerTeacher. Long term substitutes will be assigned their own logon for PowerTeacher and the network. *Student Teachers are not authorized to access PowerTeacher to enter grades since that access is granted to one, specific teacher.*

Personal devices that are used to access district resources such as email, student information systems, and other online resources must be password protected.

Users are responsible for properly logging off at the conclusion of a session and locking the computer if out of view of the computer for any period of time. Users will be held responsible for all actions taken under their user account.

> Interactive Whiteboard, TV, Projector: When a staff member is conducting a group activity using the SmartBoard, students may interact with the activity under the direct supervision of staff. The staff member must be actively engaged in the lesson. Use of devices in this manner is not permitted if a student is working independently or the staff member is working elsewhere or circulating the room.

Each user will have access to a Microsoft 365 account and/or an iCloud drive to store files. Users are not to save files to the local computer. Users must manage their file storage and email system by deleting files that are outdated or otherwise unnecessary and not required through a records retention policy. All staff are responsible for preserving files as required by the district's records retention policy.

Users may not attempt to view or configure network or system settings, files, or programs. All users are required to notify the technology department immediately of any breach, suspected breach, or potential breach of network security. The user will not demonstrate the problem to anyone outside of the technology department.

Staff will save and organize files and emails, that would otherwise be kept in a student records folder or personnel file as directed in the district's records retention policy. Staff will not disclose or release personally identifiable information about students except in accordance with the Family Educational Rights Privacy Act (FERPA) and the district's student records policy.

Sound, music, video, or any other media file accessed through district technologies must be directly related to a district assignment.

Access to social networking websites are for educational purposes only and as assigned by a teacher or staff supervisor.

Cyber bullying, creating a threat to a student, staff member or when in the school environment, that has the effect of doing any of the following: substantially interfering with a student's education, creating a threatening environment, and /or substantially disrupting the orderly operation of the school is prohibited. Please refer to Board Policy 249 at https://www.carlisleschools.org/Policy249.

If a user accidentally accesses or observes material that is objectionable, obscene, illegal, or otherwise inappropriate, he or she should immediately notify the supervising teacher or supervisor. These sites should then be reported to the Technology Director.

Users are not to disclose personal information to non-district staff such as home address, physical description, route to and from school, or any other information that could threaten the safety and security of students or staff.

Email accounts are assigned to district employees. Student teachers and contracted employees should use their college or company email address to communicate with district staff through a web-based service.

Users must not forward spam or non-work-related email to any other district or non-district account.

Video Conferencing
Video conferencing tools can be a valuable resource for virtual learning and other opportunities for students, staff, parents, and community member so meet outside of a physical space. All communication (through audio, video, still images, etc.) and behavior in a video conference follow the same expectations as in the regular face-to-face school setting.

Internet Access
The district has installed Internet site filtering software to prevent onsite, network users from accessing sites that are inappropriate for educational use. Filtering software is installed on all District-owned, student devices for internet filtering for both on-campus and off-campus access. Filtering will be updated periodically by the manufacturer of the software to include newly discovered sites that are inappropriate. The technology department in coordination with the administration will also evaluate and, if necessary, block access to reported sites and override blocked sites that are determined to be appropriate. Users may not use software, alter proxy settings, or use any other means to bypass the district filter.

Consequences for Inappropriate Use
The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of the network; intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services shall be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet or any application with messaging options, in addition to the stipulations of this policy.

The district reserves the right to enact disciplinary action in accordance with employee policies or student conduct guidelines for inappropriate, unauthorized, or illegal use of technologies. For students, disciplinary action may include suspension or expulsion. For staff, disciplinary action may include suspension or termination. The district reserves the right to charge the user for repair or replacement costs of such technologies.

Vandalism is prohibited and users will be liable for any costs associated with such an act. Vandalism includes destruction or modification to hardware as well as any malicious attempt to harm or destroy data of another user, Internet, or other networks; this includes but is not limited to uploading or creating computer viruses. Vandalism may result in loss of access privileges, disciplinary action, and/or legal proceedings.

V. Warranties
The district makes no warranties of any kind, whether expressed or implied, for the services it is providing. The district will not be responsible for any damages a user suffers. This includes loss of data resulting from delays, non-deliveries, mis deliveries, or service interruptions caused by the district's negligence or by the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The district specifically denies any responsibility for the accuracy or quality of information obtained through its services. All users need to consider the source of any information they obtain, and consider how valid the information may be.

The district will not be responsible for unauthorized charges or fees resulting from access to the Internet. All financial responsibility will rest with the individual employee or student who incurs the unauthorized charges or fees.