ABINGTON SCHOOL DISTRICT
ABINGTON, PENNSYLVANIA

SUPERINTENDENT'S ADMINISTRATIVE PROCEDURE		REGARDING:	**Acceptable Use of Technology**
Section:	**Technology**		
Effective Date:	September 10, 1997		
Reissued:	5/15/02, 8/26/08 8/9/11, 8/22/11, 6/26/12, 6/13/17, 10/16/19, 6/24/20, 8/25/22, 1/23/24, 8/16/24	See Also:	Related Board Policy; School Code: Section 4601et seq.; 20 U.S.C. Section 1232g; 18 U.S.C. Section 2510 et seq.

The following guidelines shall apply to all Users of District Technology Resources, unless otherwise specified. In addition, these guidelines shall, unless otherwise specified, be applicable to the use of all District Technology Resources, whether connected to an electronic network or operated on a stand-alone basis.

User Agreements

Students and parents/guardians will be provided annual notification of the Board Policy and Superintendent's Administrative Procedure titled "Acceptable Use of Technology."

Upon employment, staff members will be required to review the Board Policy and Superintendent's Administrative Procedure titled "Acceptable Use of Technology" and "Web Content, Hosting and Maintenance" and sign the form attached hereto as Attachment I indicating they have read, understand and agree to be bound by these documents prior to being issued or permitted to use District Technology Resources. This signed form will remain in the employee's personnel file in the Office of Human Resources. Students from colleges and universities completing an internship or student teaching in the District will be required to review the Board Policy and Superintendent's Administrative Procedures titled "Acceptable Use of Technology" and "Web Content, Hosting and Maintenance" and sign the form attached hereto as Attachment II. This signed form will remain in the student's file in the Office of Teaching and Learning.

Vendors, contractors, consultants, temporary and other non-employee workers at the District, including all personnel affiliated with third parties will be required to review the Board Policy and Superintendent's Administrative Procedure titled "Acceptable Use of Technology" and "Web Content, Hosting and Maintenance" and sign the form attached hereto as Attachment III indicating they have read, understand and agree to be bound by these documents prior to being issued or permitted to use District Technology Resources. This signed form will remain on file in the Business Office.

Access to District Technology Resources will be revoked immediately following an employee's termination, separation of employment, or conclusion of contract or agreement with the District.

General Expectations

Individual Users of the District Technology Resources are responsible for their behavior and communications while using such resources.

Users are required to comply with the provisions outlined in this Superintendent's Administrative Procedure, the accompanying Board Policy, and any user agreement signed as a condition of being given access to District Technology Resources.

Users of District Technology Resources are responsible for safeguarding their individual usernames and passwords used to access District Technology Resources. The Superintendent, Director of Information Technology, or their designee(s) may require Users to periodically change their passwords as a security enhancement measure. Administrators and personnel with access to sensitive information must employ multi-factor authentication (MFA) to secure their accounts. Compliance with MFA requirements is mandatory to ensure the protection of network resources and sensitive data.

Student Users are reminded that all Abington School District rules for appropriate student behavior and communication apply to use of District Technology Resources as they would to the classroom, school hallways, buildings, property, bus stops, etc. Users accessing District Technology Resources are responsible for their behavior and communications while using and communicating over the network. Inappropriate, unauthorized, or illegal use will result in the suspension of access privileges and appropriate student discipline.

Individuals who bring their own personal technology devices onto school property during school hours or working time, onto school vehicles, or to school-sponsored events or activities, are expected to adhere to the provisions outlined in this Superintendent's Administrative Procedure and the accompanying Board Policy.

Vendor Expectations

<u>General Requirements:</u>

- Vendor is required to develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, security, integrity and availability of all maintained or transmitted District data.
- Vendor is required to only use District data systems, resources, integrations, and access solely for the original purpose for which it was intended, as stipulated in any contract which exists between Vendor and the District.
- Vendor is prohibited from mining District data for any purpose whether internal or external to Vendor Company.
- Vendor is prohibited from sharing District data with any third party, without express permission of the District authorities in writing.
- Vendor should be aware that the data they create for District systems remains the property of the District. Because of the need to protect the District's network, management cannot guarantee the confidentiality of information stored on any network devices not belonging to the District.

- Vendor is responsible for exercising good judgment regarding appropriate use of District Technology Resources in accordance with District policies, standards, and guidelines. District Technology Resources may not be used for any unlawful or prohibited purpose.
- For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic. Vendor devices that interfere with other devices or users on the District network may be disconnected without warning.

Vendors Requiring Systems Accounts

- Vendor is responsible for the security of data, accounts, and systems under their control. Vendor must keep passwords secure and not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual(s), either deliberately or through failure to secure its access, is a violation of this policy.
- Vendor must maintain system-level and user-level passwords in accordance with District standards maintained by the Office of Information Technology.
- Vendor must ensure through legal or technical means that proprietary information remains within the control of the District at all times. Conducting District business that results in the storage of proprietary information on personal or non-District controlled environments, including devices maintained by third party with whom the District does not have a contractual agreement, is prohibited. This specifically prohibits the use of an email account that is not provided by the District, or its partners, for school business.

Vendors Requiring Computing Assets

- Vendor is responsible for ensuring the protection and security of the assigned ASD assets that includes reasonable protection from any environmental elements. Promptly report any theft of District assets to the immediate supervisor or manager.
- All District Technology Resources must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. Vendor must lock the screen or log off when the device is unattended.
- Vendor must not interfere with District device management or security system software, including, but not limited to, antivirus, security updates, and software distribution.
- Devices that connect to the District network must comply with the Network Use detailed on the next section.

Enforcement

Any violation of this policy may result in termination of services, access, or agreements with Vendor, and be subject to additional actions which may be detailed in the contractual agreement between Vendor and the District.

No Expectation of Privacy

Users of District Technology Resources are reminded that there shall be no expectation of privacy in internet/network activity in connection with the use of District Technology Resources. Files or other information placed or stored on District Technology Resources are subject to review and may be deleted without notice. Routine maintenance or monitoring may lead to discovery that a User has or is violating the requirements of this Superintendent's Administrative Procedure or the accompanying Board Policy. A specific search of an individual

User's account(s) may be conducted if there is reasonable suspicion that a User has violated the law, Board Policy, or this Superintendent's Administrative Procedure. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.

Internet Filtering

The District is committed to the filtering of Internet resources through the purchase and application of standard filtering software to protect minor students from obscene material, pornography, including, but not limited to, child pornography, and other visual depictions deemed harmful to minors, as defined by the Children's Internet Protection Act (CIPA). Staff, students, and parents/guardians are advised, however, that no filtering software is completely secure or effective. An administrator, supervisor, or other person authorized by the Superintendent or Director of Information Technology may disable the filtering software if needed for bona fide research or another lawful purpose. While the District reserves the right to adjust or enhance its filtering, it is not in a position to make such adjustments or enhancements on an individual student basis at the request of a parent/guardian. Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this Superintendent's Administrative Procedure or the accompanying Board Policy. The District reserves the right to monitor and restrict or prohibit access to websites including:

- Websites primarily intended to facilitate illegal activity
- Social media
- Websites that promote obscene, pornographic or salacious material
- Websites that pose a threat to the network hardware and software
- Websites that promote drugs and drug paraphernalia
- Websites that promote hate speech and hate groups
- Websites that promote terrorism, weapons and manufacture of explosives
- Auction websites
- Adware
- Proxy sites or services that mask web traffic
- Other categories as determined by the Superintendent or designee

In compliance with the Children's Internet Protection Act (CIPA), the District will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms as well as cyber bullying awareness and response. Such instruction will take place on an annual basis.

Limitation of Liability

The availability of electronic information through District Technology Resources does not imply endorsement of the content by the District nor does the District guarantee the accuracy of information received through the District Technology Resources or that use will be error free or uninterrupted. The District shall not be liable for any direct, incidental, or consequential damages sustained or incurred in conjunction with the use, operation or inability to access or use District Technology Resources, including the loss of data, information or anything else of value.

The District shall not be liable for any damage incurred due to harmful programs or materials (including computer viruses), which may be accessible or propagated through District Technology Resources. The District shall not be responsible for any unauthorized financial obligations resulting from access to District Technology Resources.

Since the network and network storage areas are District property or otherwise constitute District-leased storage capacity, network administrators may review and delete files, web browsing history and communications to maintain system integrity and ensure that the system is being used in accordance with established responsible use guidelines. Users should not expect that files or other electronic information stored on or available through District servers will be private or secure.

Users will be required to indemnify the District against any damage caused by the User's inappropriate use of District Technology Resources.

Responsible Use Standards / Prohibited Activities

The following actions while using District Technology Resources shall constitute a violation of Abington School District's responsible use standards:

- Using District Technology Resources for illegal activities, including, but not limited to, communicating transmitting, or accessing defamatory, threatening, racially offensive, sexually explicit, obscene, pornographic, or otherwise inappropriate materials
- Unauthorized installation, distribution, reproduction, or use of copyrighted materials, including, but not limited to, pictures, music, video, and software
- Unauthorized access or attempts to gain unauthorized access to District Technology Resources, including, but not limited to, hacking, bypassing security measures, and accessing or modifying files or data without consent
- Unauthorized sniffing of network traffic or scanning of District Technology Resources for system vulnerabilities
- Disruption of normal operations or the work of others, including, but not limited to, activities such as ICMP loss, packet spoofing, denial of service, heap or buffer overflows, forged routing information, introducing honeypots or honey nets, destruction of data, spreading computer viruses, worms, or other malware, or sending spam via email, text messages, pages, instant messaging, or voice mail
- Uploading or downloading games, programs, files, or other electronic media absent permission from the Director of Information Technology or designee. Teachers who receive requests from students to upload or download games, programs, files, or other electronic media shall direct such requests to the Director of Information Technology or designee
- Destruction, modification, unauthorized repair, vandalism or abuse of District Technology Resources
- Unauthorized establishment of websites linked to District websites or themselves purporting to be District-affiliated websites and social media groups
- Communicating threats to the welfare of the school community, school property, or any individual
- Using District Technology Resources to transmit or engage in hate speech, defamation, discrimination, harassment, bullying, cyberbullying, hazing, or any other objectionable, offensive, or inflammatory communication under Board Policy or applicable law

- Forging, misrepresenting, obscuring, suppressing, spoofing or impersonating another user or quoting personal communications in a public forum without the original author's or user's prior consent
- Using District Technology Resources for unauthorized fundraising, solicitation, commercial purposes, product advertising, or political and religious proselytizing or lobbying
- Use of a District email or other communication mechanisms to engage in conduct that violates District policies or guidelines
- Use of the Internet or District network that violates the Pennsylvania Child Internet Protection Act (CIPA)
- Posting to a public newsgroup, bulletin board, or listserv with a District account represents the District to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the District

Other actions in violation of school rules, Board Policy or any accompanying Superintendent's Administrative Procedure, directives or regulations of the Superintendent, Director of Information Technology, or their designee(s) regarding appropriate use of District Technology Resources, any applicable code of conduct or collective bargaining agreement, or any local, state or federal law.

Users of District Technology Resources shall promptly report violations of this Superintendent's Administrative Procedure or the accompanying Board Policy to their teacher, building principal or supervisor.

Users of District Technology Resources shall immediately notify their teacher, building principal, supervisor or the Director of Information Technology or designee if they have identified a possible security threat or breach.

If a User of District Technology Resources inadvertently accesses any inappropriate material, as described above, they shall immediately disclose the inadvertent access to their teacher, supervisor or building principal. This will protect such User from an allegation that they intentionally violated this Superintendent's Administrative Procedure or the accompanying Board Policy.

Consequences of Misuse of District Technology Resources

The use of District Technology Resources is a privilege, not a right, which may be revoked at any time for violation of the terms outlined in this Superintendent's Administrative Procedure or the accompanying Board Policy.

Misuse of District Technology Resources or other violation of this Superintendent's Administrative Procedure or the accompanying Board Policy may lead to disciplinary action in accordance with school rules, Board Policy, applicable Superintendent's Administrative Procedures, and any applicable collective bargaining agreement. Such action could include, but is not limited to, usage restrictions, loss of access privileges, suspension, expulsion, termination, restitution, referral to law enforcement, and/or any applicable consequence outlined in a student handbook, collective bargaining agreement, or Board Policy/SAP, as appropriate under the circumstances.

The District will cooperate fully with local, state and federal officials in any investigation conducted concerning or related to illegal activities of any individuals misusing the District's network or telecommunications resources/devices. In the event there is an allegation that a staff member has engaged in conduct or communication in violation of this Superintendent's Administrative Procedure or the accompanying Board Policy, the staff member will be provided with a written notice of the alleged violation and be given an opportunity to present an explanation. Any District-initiated disciplinary action(s) will be tailored to meet specific concerns related to the violation.

Employee Use of Personal Devices to Conduct School District Business

Should an employee elect to use a personal technology device, such as a mobile phone or tablet, to access District Technology Resources, such as their District-issued email account, the employee shall use a PIN, passcode, or password to protect their device. The District reserves the right to configure access to District Technology Resources to require the use of a PIN, passcode, or password in order to access District Technology Resources.

Should an employee's personal technology device that is or has been used to access District Technology Resources become lost or stolen, the employee shall promptly advise the Director of Information Technology or designee so that appropriate steps can be taken to minimize the risk of the unauthorized disclosure of confidential student or personnel information.

PARENTAL NOTIFICATION

Online and printed materials will notify parents and guardians of student access to District Technology Resources. Alternate arrangements will be made for any student whose parents/guardians advise the principal that they decline participation for their child.

Attachment I

ABINGTON SCHOOL DISTRICT
Abington, Pennsylvania

STAFF NETWORK AND TELECOMMUNICATIONS RESOURCES AGREEMENT FORM

This Section Must Be Signed by the Staff Member:

I have read, I understand, and I will abide by the Abington School District Board Policy and Superintendent's Administrative Procedure titled "Acceptable Use of Technology" as well as the Board Policy and Superintendent's Administrative Procedure titled "Web Content, Hosting and Maintenance."

Name of Abington School District Staff User: _____

Abington School District Staff User Signature: _____

Date: _____

SUBMIT THIS FORM TO THE OFFICE OF HUMAN RESOURCES

Attachment II

ABINGTON SCHOOL DISTRICT
Abington, Pennsylvania

INTERN/STUDENT TEACHER NETWORK AND TELECOMMUNICATIONS RESOURCES AGREEMENT FORM

This Section Must be Completed and Signed by the Intern/Student Teacher:

I am requesting access to the Abington School District network for the duration of my internship/student teaching placement. I have read, I understand, and I will abide by the Abington School District Board Policy and Superintendent's Administrative Procedure titled "Acceptable Use of Technology" as well as the Board Policy and Superintendent's Administrative Procedure titled "Web Content, Hosting and Maintenance."

Name: _____

College/University: _____

ASSIGNMENT IN ABINGTON SCHOOL DISTRICT:

School: _____

Assignment: _____

Dates of the Assignment: From_____To: _____

Cooperating Supervisor: _____

Signature: _____

Date: _____

SUBMIT THIS FORM TO THE OFFICE OF TEACHING AND LEARNING

Attachment III

ABINGTON SCHOOL DISTRICT
Abington, Pennsylvania

VENDOR NETWORK AND TELECOMMUNICATIONS RESOURCES AGREEMENT FORM

This Section Must be Completed and Signed by the VENDOR:

I have read, I understand, and I will abide by the Abington School District Board Policy and Superintendent's Administrative Procedure titled "Acceptable Use of Technology" as well as the Board Policy and Superintendent's Administrative Procedure titled "Web Content, Hosting and Maintenance."

To be completed by the Vendor:

Name of Vendor: _____

Name of Account Holder: _____

Title of Account Holder: _____

Signature: _____

Date: _____

Name of Manager/Supervisor: _____

Title of Manager/Supervisor: _____

Signature: _____

Date: _____

To be completed by Abington School District:

Name: _____

Department: _____

Signature: _____

Date: _____

Date Access Ends: _____

SUBMIT THIS FORM TO THE BUSINESS OFFICE
WITH A COPY SENT TO THE OFFICE OF INFORMATION TECHNOLOGY