No. 815
Montoursville Area School
District Administrative
Guidelines

ACCEPTABLE USE OF TECHNOLOGY

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.

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 Administrative Guideline, 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 user names and passwords used to access District technology resources. The Superintendent, Supervisor of Information Technology, or their designee(s) may require users to periodically change their passwords as a security enhancement measure.

Student users are reminded that all school rules for appropriate student behavior and communication apply when using District technology resources, as they would in the classroom, school hallways, buildings, property, bus stops, etc. Inappropriate, unauthorized, or illegal use will result in 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 Administrative Guideline and the accompanying Board Policy.

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.

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 are advised, however, that no filtering software is completely secure or effective. Merely because a technology protection measure does not prevent access to a particular site or to particular materials does not indicate that the site or the materials are appropriate. The District encourages parents/guardians to specify to their child(ren) what material is and is not acceptable to access through District technology resources, within the parameters of this Administrative Guideline and the accompanying Board Policy.

An administrator, supervisor, or other person authorized by the Superintendent or Supervisor 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 Administrative Guideline or the accompanying Board Policy.

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, which shall include a discussion about cyber bullying awareness and response. Information will be approved annually as part of the student handbooks.

Limitation of Liability

The District does not warrant that the use of specific District technology resources will meet any specific requirements, or that they 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 financial obligations arising out of the unauthorized use of District technology resources.

Responsible Use Standards / Prohibited Activities

The following actions while using District technology resources shall constitute a violation of the District's responsible use standards:

1. Using District technology resources to engage in, facilitate or promote illegal activity;
2. Communicating threats to the welfare of the school community, school property, or any individual;
3. Using District technology resources for fundraising purposes, unless otherwise permitted by Board Policy or authorized in advance by the Superintendent or designee;
4. Using District technology resources for commercial or for-profit purposes, unless otherwise permitted by Board Policy or authorized in advance by the Superintendent or designee;
5. Using District technology resources to promote or participate in gambling, gaming, or betting activities, other than those related to a legitimate school assignment, project or job responsibility;
6. Using obscene, inappropriate or profane language;
7. Accessing, sending, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal or inappropriate materials, images or photographs;
8. Using District technology resources to transmit hate mail/speech, communication deemed to constitute defamation or discrimination under Board Policy or applicable law, or threatening, racially offensive, or sexually explicit material;
9. Engaging in conduct that constitutes unlawful harassment, bullying, cyberbullying, or hazing under Board Policy or applicable law;
10. Sharing confidential student or personnel information without appropriate authorization;
11. Sharing account passwords and electronic access with others;
12. Using, or allowing another to use, a user name, account or password not their own;

13. Using District technology resources for campaigning or political activities not permitted by other Board Policy;
14. Destruction, unauthorized modification or repair, vandalism, or abuse of District technology resources;
15. Unauthorized access (i.e. hacking) or exceeding the scope of one's authorized access, including trespassing in another's user account, folders, work or files;
16. Attaching unauthorized external devices to District technology resources;
17. Attempting to circumvent system security, guess passwords, bypass firewall, web filtering or anti-virus systems, or in any way gain unauthorized access to District technology resources;
18. Unauthorized scanning of District technology resources for system vulnerabilities;
19. Unauthorized or illegal installation, distribution, reproduction or use of copyrighted materials;
20. Intentionally wasting limited resources such as network bandwidth or storage, paper, toner, and other supplies;
21. Using District technology resources to disrupt the work of others or normal school operations;
22. Impersonation of another user or quoting personal communications in a public forum without the original author's prior consent;
23. Representing personal views as those of the District;
24. Using District technology resources to intentionally obtain or modify files, passwords, or other data belonging to another;
25. Uploading or downloading games, programs, files, or other electronic media absent permission from the Superintendent, Supervisor of Information Technology, building principal, or their designee(s). Teachers who receive requests from students to upload or download games, programs, files, or other electronic media shall direct such requests to the Supervisor of Information Technology or building principal;
26. Making deliberate attempts to disrupt the performance of District technology resources or destroy data by spreading computer viruses, worms, or other malware;
27. Unauthorized establishment of websites linked to District websites or themselves purporting to be District-affiliated websites and social media groups; and
28. Engaging in any conduct that violates school rules, Board Policy or any accompanying Administrative Guideline, directives or regulations of the Superintendent, Supervisor of Information Technology, or their designee(s) regarding appropriate use of District technology resources, any applicable code of conduct, student or staff handbook, collective bargaining agreement, or any local, state or federal law.

Users of District technology resources shall promptly report violations of this Administrative Guideline or the accompanying Board Policy to their teacher, building principal or immediate supervisor.

Users of District technology resources shall immediately notify their teacher, building principal or Supervisor of Information Technology 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 Administrative Guideline 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 Administrative Guideline or the accompanying Board Policy.

Misuse of District technology resources or other violation of this Administrative Guideline or the accompanying Board Policy may lead to disciplinary action in accordance with school rules, Board Policy, applicable Administrative Guidelines, 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, code of

conduct, collective bargaining agreement, staff handbook, or Board Policy/Administrative Guideline, as appropriate under the circumstances.

User Agreements

District employees must sign a User Agreement **(See Attachment A)** indicating that they have read, understand and agree to be bound by this Administrative Guideline and the accompanying Board Policy, or otherwise acknowledge being bound by this Administrative Guideline and the accompanying Board Policy through other means, prior to being issued or permitted to use District technology resources.

Students must sign a User Agreement **(See Attachment B)** indicating that they have read, understand and agree to be bound by this Administrative Guideline and the accompanying Board Policy prior to being issued or permitted to use District technology resources.

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 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 Technology Department so that appropriate steps can be taken to minimize the risk of the unauthorized disclosure of confidential student or personnel information.

Individualized Searches of District Technology Resources

If the District has reasonable suspicion that a user of District technology resources has violated the terms of this Administrative Guideline or the accompanying Board Policy, an individualized search of the user's network account, email system, or other District technology resource may be conducted.

The nature and scope of any investigation or individualized search will be reasonable in the context of the alleged violation.

The user will be provided with notice of the alleged violation and be given an opportunity to present an explanation. Nothing in this provision shall preclude authorized District employees from conducting routine monitoring or maintenance of District technology resources, as contemplated in this Administrative Guideline and the accompanying Board Policy, without prior notice.

Procedure for Individualized Searches of District Technology Resources

Upon reasonable suspicion that a user of District technology resources has violated or is violating the terms of this Administrative Guideline or the accompanying Board Policy, the matter shall be reported to the Superintendent , who shall report the suspected violation to the Supervisor of Information Technology.

If the Supervisor of Information Technology determines that the user's network account or other District technology resource should be accessed and/or searched, the following procedures shall take place:

1. If the suspected violation is believed to be criminal in nature or it is suspected that evidence of a crime is on the network account or other District technology resource, the Supervisor of Information Technology shall contact law enforcement to report the incident. If law enforcement

indicates it will conduct an investigation, the Supervisor of Information Technology shall take all reasonable steps to comply with the investigation. If the law enforcement investigation reveals evidence of conduct that constitutes a violation of this Administrative Guideline or the accompanying Board Policy, the District may initiate appropriate disciplinary procedures.

2. If the suspected violation is believed not to be criminal in nature, but related to a violation of this Administrative Guideline or the accompanying Board Policy, then the Supervisor of Information Technology will determine whether to search the user's network account or other District technology resource. This determination will be made as follows:
    a. Where the suspected violation in any way involves sexually explicit visual depictions of students or other individuals under 21 years of age, no search may be performed by District personnel, and the matter must be referred to law enforcement for appropriate action.

3.
    b. For offenses that do not involve sexually explicit visual depictions of students or other individuals under 21 years of age, the decision to search a user's network account or other District technology resource shall be guided by the following considerations:
        i. the anticipated ease or difficulty of locating the evidence of the suspected wrongful activity;
        ii. the likelihood that such a search would materially modify or destroy the evidence of suspected wrongful activity; and
        iii. the immediacy of the need for identifying the evidence of suspected wrongful activity.

4.
    c. If the Supervisor of Information Technology determines that an in-house search is appropriate, they will generally identify the suspected violation and conduct a search limited in scope based upon the nature of the suspected violation, tailored to identify evidence of the suspected violation.

1. d. If evidence of a violation is identified, the Supervisor of Information Technology will take reasonable measures to preserve the evidence pending the results of any disciplinary proceedings.

1. e. If evidence of a violation is not located, but the Supervisor of Information Technology believes that a forensic investigation would reveal evidence of a violation, then they may arrange such a forensic investigation.

1. f. If evidence of a violation is not located and the Supervisor of Information Technology believes that there is no reason to believe that a forensic investigation would reveal such evidence, then no further action will be taken.

1. g. If, in the course of conducting the limited search contemplated above, the Supervisor of Technology discovers information which they reasonably believes is evidence of a crime, they should immediately stop the search, contact law enforcement, and take all reasonable steps to comply with any subsequent law enforcement investigation.

1. h. If, in the course of conducting the limited search contemplated above, the Supervisor of Information Technology views information that provides reasonable suspicion that an additional or different violation of this Administrative Guideline or the accompanying Board Policy has occurred or is occurring, they can expand the scope of the search, as appropriate, based upon the further reasonable suspicion or, if the reasonable suspicion relates to suspected criminal activity, stop the search and report the matter to law enforcement.

1:1 Technology Agreement

Technology equipment provided as part of the district's 1:1 initiative is the property of Montoursville Area School District (MASD) and is being supplied for **STUDENT USE ONLY**. All equipment must be returned at a designated time or upon request of the district.

Any student who is no longer enrolled at Montoursville Area School District is required to return the equipment they have been provided.

If a Device and AC Adapter are not returned at a designated time, action will be taken to recover the device and/or the cost of the device through all legal options.

**If the equipment is not returned, it will be remotely locked by the district which will make the device inoperable.*

Parents/ Guardians are responsible for ensuring the provided equipment is used appropriately and cared for.

By accepting the device, you are taking responsibility for all the statements listed below:

1. I will care for the provided device and ensure that it is retained in a safe environment. This device is, and at all times, remains the property of MASD of Montoursville, PA and is herewith lent to the student for educational purposes only. Students may not deface or destroy this property in any way. Inappropriate use of the equipment may result in the student losing the right to use this equipment.
2. If at any time the device is damaged (due to misuse), lost, or stolen, made unserviceable, or not returned at the appropriate time, you will be billed for the replacement of the equipment at market value.
3. The MASD property may be used by students only for educational purposes in accordance with the school district's policies and rules, as well as local, state, and federal statutes. Students may not install or use any software other than the software owned, installed, and approved by MASD. If students attempt to bypass the internet filter, they will face disciplinary action.
4. Identification and inventory have been taken of the devices. Additional identification tags such as stickers, labels, tags, or markings are not to be added to the device without prior approval from MASD.
5. I acknowledge and agree that the device is subject to inspection at any time without notification. If requested by MASD, you will make the device available for inspection and will comply with any and all investigatory procedures in accordance with MASD policies and procedures as well as local, state, and federal statutes.

STUDENT USER AGREEMENT

When using District technology resources, students are required to adhere to the terms and conditions contained in School Board Policy and Administrative Guideline 815 (Acceptable Use of Technology), which are available for review on the District's website.

Prior to being issued or permitted to use District technology, students are required to complete and return this this form acknowledging and agreeing to be bound by the District's acceptable use of technology standards.

By signing below, the Student acknowledges as follows:

1. I have reviewed the Montoursville Area School District's Board Policy and Administrative Guideline 815 (Acceptable Use of Technology), recognize its importance, and agree to be bound by the terms and conditions outlined therein when using District technology resources.

2. I understand that if I violate Board Policy or Administrative Guideline 815, I will be subject to school-based discipline, which could include, but is not necessarily limited to, usage restrictions, loss of access privileges, suspension, expulsion, restitution, referral to law enforcement, and/or any applicable consequence outlined in the student handbook or any other Board Policy or Administrative Guideline, as appropriate under the circumstances.

3. I agree to promptly report violations of the District's acceptable use of technology standards to my teacher or building principal.

4. I understand that the District regularly monitors internet/network activity in connection with the use of District technology resources, and that there shall be no expectation of privacy in such activity.

5. I acknowledge and agree that the use of the MASD device is a privilege and agree to the terms on laid out in form 815C (1:1 Technology Agreement). I acknowledge responsibility to protect and safeguard the MASD property and return the device to MASD in good condition and repair.

Student's Name:_____Date: _____

Student Signature: _____

Parent's Signature (For Students Under 18): _____