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 Regulation, the accompanying Board Policy, and any user agreement signed or acknowledged as a condition of being given access to District technology resources.

Users of District technology resources are responsible for safeguarding their user names and passwords used to access District technology resources. The Superintendent, Director of Educational Program, 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. Therefore, the term "reasonable suspicion" when used in this regulation will have the same meaning as the definition in other policies and regulations related to student searches as cross-referenced below.

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 Regulation and the accompanying Board Policy, as well as any other Policy or Administrative Regulation governing the use of such personal devices.

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 effective. 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 Regulation and the accompanying Board Policy.

An administrator, supervisor, or other person authorized by the Superintendent or Director of Educational Program 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 able to make such adjustments or enhancements on an individual student basis at the request of a parent/guardian.

Upon request, 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 Regulation or the accompanying Board Policy.

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.

Acceptable Use Standards / Prohibited Activities

The following actions while using District technology resources, while not necessarily an exhaustive list, shall constitute a violation of the District's acceptable use standards:

a. Using District technology resources to engage in, facilitate, or promote illegal activity;
b. Communicating threats to the school community, school property, or any individual;
c. Using District technology resources for fundraising purposes, unless otherwise permitted by Board Policy or authorized in advance by the Superintendent or designee;
d. 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;
e. Using District technology resources to promote, facilitate, or participate in gambling, gaming, or betting activities, other than those related to a legitimate school assignment, project or job responsibility;
f. Using obscene, inappropriate or profane language;

g. Accessing, sending, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal or inappropriate materials, images or photographs;
h. 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;
i. Engaging in conduct that constitutes discriminatory harassment, bullying, cyberbullying, or hazing under Board Policy or applicable law;
j. Sharing confidential student or personnel information without appropriate authorization;
k. Sharing account passwords with others;
l. Using, or allowing another to use, a username, account or password not their own;
m. Using District technology resources for campaigning or political activities not permitted by other Board Policy;
n. Destruction, unauthorized modification or repair, vandalism, or abuse of District technology resources;
o. 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;
p. Attaching unauthorized external devices to District technology resources;
q. 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;
r. Unauthorized scanning of District technology resources for system vulnerabilities;
s. Unauthorized or illegal installation, distribution, reproduction or use of copyrighted materials;
t. Intentionally wasting limited resources such as network bandwidth or storage, paper, toner, or other supplies;
u. Using District technology resources to disrupt the work of others or normal school operations;
v. Impersonation of another user or quoting personal communications in a public forum without the original author's prior consent;
w. Representing personal views as those of the District;
x. Using District technology resources to intentionally obtain or modify files, passwords, or other data belonging to another;
y. Uploading or downloading games, programs, files, or other electronic media absent permission from the Superintendent, Director of Educational Program or building principal. 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 Educational Program or designee, or building principal;
z. Making deliberate attempts to disrupt the performance of District technology resources or destroy data by spreading computer viruses, worms, or other malware;
aa. Unauthorized establishment of websites linked to District websites or themselves purporting to be District-affiliated websites and social media groups;
bb. Engaging in any conduct that violates school rules, Board Policy or any accompanying Administrative Regulation, directives or regulations of the Superintendent, Director of Educational Program, 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 Administrative Regulation 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, immediate supervisor, or the Director of Educational Program 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, immediate supervisor or building principal. The teacher, immediate supervisor or building principal shall notify the Director of Educational Program of any such incidents.

District-Issued Email – Use and Standardization

Employees are expected to use their District-issued emails in their professional capacity only. For example, while District employees communicate over email about a wide variety of subjects in the course of their work, all communication over District-issued email must still fall within the grounds of the District's Acceptable Use Standards. This includes adhering to the prohibition on the promotion of religion, partisan political messaging, and other prohibited activities listed in this regulation.

Within the limits of the law, the District strives to create an environment that fosters free expression of religion. Subject to employees' constitutional right to freedom of religious expression, District employees may not use district technology or accounts to promote a particular religious order, sect, denomination, or belief. This includes text or images contained within email signatures, usernames, or other profiles associated with district accounts.

Similarly, employees who are acting on behalf of the District or a school, or who are reasonably perceived to be representing the District or a school, must maintain political neutrality in their use of District technology and accounts. This includes text or images contained within email signatures, usernames, or other profiles associated with District accounts. In case of doubt as to whether this part of the regulation applies to a specific text or image, employees should contact the employee's supervisor or the Director of Human Resources.

Signature Block

District employees may choose to use a signature block. Signature blocks shall be restricted to the employee's information, which at the employee's discretion may include name, position, pronouns, contact information, and school name if relevant.

Employees may not add additional text, such as quotes, or images to their signature block in their District-issued emails. The District reserves the right to adjust what information is permitted in the signature block as needed and consistent with the standards of political and religious neutrality and other expression contained in this and other District policies and regulations cross-referenced below.

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 Regulation or the accompanying Board Policy

Misuse of District technology resources or other violation of this Administrative Regulation or the accompanying Board Policy may lead to disciplinary action in accordance with school rules, Board Policy, applicable Administrative Regulations, 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/Administrative Regulation, as appropriate under the circumstances.

User Agreements

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

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

Employee Use of Personal Devices to Conduct District Business

Employees are discouraged, but not prohibited, from using a personal electronic device, such as a mobile phone, tablet, or computer, to access District technology resources, as long as the employee uses a PIN, passcode, or password to protect their device. Employees shall not store any personally identifiable or sensitive information on personally owned devices at any time.

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.

Periodic Random Search of Network User Activity on District Technology Resources

It is impractical and cost-prohibitive for the District to review every network user's use of District technology resources to determine if a network user is engaging in improper or harmful activity. However, the District may from time-to-time conduct random searches of network users' activity on District technology resources using search techniques reasonably designed to discover improper or harmful activity by students or other users. If a periodic random search results in reasonable suspicion for a more expansive search, then the procedures outlined in this Regulation regarding the Procedure for Individualized Searches of District Technology Resources applies.

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 Regulation or the accompanying Board Policy, a further 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.

Nothing in this provision shall preclude authorized District employees from conducting routine monitoring or maintenance of District technology resources, as contemplated in this Administrative Regulation 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 Regulation or the accompanying Board Policy, the matter shall be reported to the Director of Educational Program, or to the appropriate administrator or building principal who shall report the suspected violation to the Director of Educational Program.

If the Director of Educational Program, in consultation with the Superintendent and/or the District Solicitor, 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 in any way involving sexually explicit visual depictions of students or other individuals under 21 years of age, the Director of Educational Program shall contact law enforcement to report the incident. If law enforcement indicates it will conduct an investigation, the Director of Educational Program 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 Policy or the accompanying Administrative Regulation, 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 Policy or the accompanying Administrative Regulation, then the Director of Educational Program will determine whether to search the user's network account or other District technology resource, in consultation with the Superintendent and/or District Solicitor. This determination will be made as follows:

    a. 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.
    b. If the Director of Educational Program 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.
    c. If evidence of a violation is identified, the Director of Educational Program will take reasonable measures to preserve the evidence pending the results of any disciplinary proceedings.
    d. If evidence of a violation is not located, but the Director of Educational Program believes that a forensic investigation would reveal evidence of a violation, they may arrange such a forensic investigation.
    e. If evidence of a violation is not located and the Director of Educational Program believes that there is no reason to believe that a forensic investigation would reveal such evidence, then no further action will be taken.
    f. If, in the course of conducting the limited search contemplated above, the Director of Educational Program discovers information which they reasonably believe 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.

g. If, in the course of conducting the limited search contemplated above, the Director of Educational Program views information that provides reasonable suspicion that an additional or different violation of this Administrative Regulation 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.

Cross References:

Policy and Regulation No. 4035 “Dress and Appearance”

Policy and Regulation No. 4022 “Addressing Employee Concerns and Criticism”

Policy and Regulation No. 5412 “Searches”

Adopted: October 25, 2021
Revised: January 4, 2022
Revised: September 6, 2022
Revised: January 4, 2023

Revised: August 16, 2023

Attachment A
Regulation 8080 - Acceptable Use of Technology

EMPLOYEE USER AGREEMENT

When using District technology resources, District employees are required to adhere to the terms and conditions contained in Board Policy and Administrative Regulation 8080 (Acceptable Use of Technology), which are available for review on the District's website.

Prior to being issued or permitted to use District technology resources, District employees are required to complete and return this this form (or otherwise acknowledge its content electronically) acknowledging and agreeing to be bound by the District's acceptable use of technology standards.

By signing below or otherwise acknowledging the content of this Agreement, I acknowledge as follows:

1. I have reviewed the Tredyffrin/Easttown School District's Board Policy and Administrative Regulation 8080 (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 Regulation 8080, I will be subject to discipline, which could include, but is not necessarily limited to, usage restrictions, loss of access privileges, suspension, termination, restitution, referral to law enforcement, and/or any applicable consequence outlined in Board Policy, any applicable Administrative Regulation, my employee handbook, or the applicable collective bargaining agreement, as appropriate under the circumstances.
3. I agree to promptly report violations of the District's acceptable use of technology standards to my immediate supervisor 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.

Employee Name: _____

Date: _____

Employee Signature: _____

Attachment B
Regulation 8080 - Acceptable Use of Technology

STUDENT USER AGREEMENT

When using District technology resources, students are required to adhere to the terms and conditions contained in Board Policy and Administrative Regulation 8080 (Acceptable Use of Technology), which are available for review on the District's website.

By signing below or otherwise acknowledging the content of this Agreement, I acknowledge as follows:

1. I have reviewed the Tredyffrin/Easttown School District's Board Policy and Administrative Regulation 8080 (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 Regulation 8080, 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 Board Policy, any applicable Administrative Regulation, or the student handbook, 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.