Administrative Procedures for Acceptable Use of Internet, Technology, and Network Resources

(Attachment for Policy No. 815)

Purpose

These Administrative Procedures are directed to employees, contractors, students, parents/guardians, and other authorized parties who use internet, technology, and/or network resources managed by the School District of Philadelphia ("District"). The goal is to provide clear expectations to all parties regarding the use of District internet, technology, and/or network resources.

Definitions

Acceptable Use Agreement (AUA): An electronic agreement that establishes the rules and guidelines that govern use of District technology resources, including but not limited to, District internet, applications and systems, and other technologies. An AUA must be reviewed and accepted by any authorized user accessing a District-issued account through a web portal (e.g., District staff, students, guardians) in order to be granted access to the system.

Website Publisher/Web Publisher: Any District staff member who has completed the necessary website accessibility training and been granted access to one or more District websites for content creation and management purposes.

Procedures

Acceptable Use Agreements

Acceptable Use Agreements (AUA) are issued electronically to **all authorized users** who access District systems using a web portal, including the Employee Portal, Student Portal, and Parent Portal. Review and acceptance of the appropriate AUA is required at the following times:

1. The first time an authorized user logs into their District-managed account
2. The start of each school year on or around September 1.

Failure to accept an Acceptable Use Agreement will result in an inability to access all District systems and technology resources.

AUAs are managed for three major user groups who review and agree via the following web portals:

- Students via the Student Portal
- Staff (Employees, Non-District staff, other authorized users) via the Employee Portal
- Guardians via the Parent Portal

Below are the key tenets for acceptable use within each population.

Students

1. **Understand and Respect Rules:** Students should understand and adhere to the rules set forth in the Acceptable Use Policy (AUP), including those related to privacy, safety, and respect for others. Students should also keep in mind that the District's Student Code of Conduct may also apply to online behaviors both in and out of school per the Student Code of Conduct.
2. **Secure Personal Information:** Students should protect their personal information and not share login credentials or other sensitive details with others.
3. **Cyberbullying:** Students must understand that cyberbullying will not be tolerated, and that they should report any instances they encounter to a teacher or other school staff member. Students may also make a report following the protocols found on the Bullying, Harassment, and/or Discrimination reporting website: https://www.philasd.org/studentrights/bhd/.

Links to Student Acceptable Use Agreements by Grade Band
Grades K - 2: IN DEVELOPMENT FOR AUGUST 2024
Grades 3 - 5: IN DEVELOPMENT FOR AUGUST 2024
Grades 6 - 8: IN DEVELOPMENT FOR AUGUST 2024
Grades 9 - 12: IN DEVELOPMENT FOR AUGUST 2024

Staff

1. **Model Good Behavior:** Teachers, school staff, and any other District staff in routine contact with students should model appropriate and safe online behavior for students.
2. **Data Privacy:** Staff must adhere to applicable guidelines, Internet Privacy Policy, student data privacy recommendations, and Board Policies (e.g. Policy 216-Student Records, Policy 324- Personnel Files) and protect the privacy of student and employee data at all times, only accessing and sharing data as required by their role. Administrators should understand their role in data governance, ensuring data is managed and used in a way that complies with legal and ethical obligations, and promoting a culture of data security within the District.
3. **Multi-Factor Authentication and Secure Access**: Staff who have access to sensitive student data either through the Student Information System, or Easy IEP should enable and utilize this service to protect against cyber security threats. You can set up multi-factor authentication here: https://www.philasd.org/technologyservices/mfa/ Staff are also expected to use strong, unique passwords.
4. **Reasonable Usage of District Technology Resources:** Usage of streaming services is largely prohibited at the District. Use of YouTube and similar services should be limited to instructional and educational needs. Please also be aware that personal licenses for streaming services may restrict certain uses of these services in certain situations (i.e. using Netflix in a classroom).

Link to Employee Acceptable Use Agreement: IN DEVELOPMENT FOR AUGUST 2024

Guardians

1. **Model Good Behavior:** Guardians should model appropriate and safe online behavior for their children.
2. **Secure Personal Information and Student Information:** Guardians should protect their personal information and the personal information and educational data of children they have authorized access to. Guardians should not share login credentials or other sensitive details with others.

Link to Guardian Acceptable Use Agreement: IN DEVELOPMENT FOR AUGUST 2024

Guidelines for Digital Citizenship

1. **Digital Etiquette:** Users must understand the need for respectful and responsible behavior when interacting with others online. This includes avoiding behaviors such as cyberbullying, posting disrespectful comments, and intentionally spreading false information. Some lapses in digital etiquette may give rise to discipline.
2. **Privacy and Security:** Users should be good stewards of digital information being shared online and only make files available to those with an explicit need to know. They should use strong, unique passwords and keep them confidential.
3. **Intellectual Property and Copyright:** Users must respect the intellectual property of others and not share copyrighted material without permission, and properly citing sources when using others' work. See Policy 814- Copyright Material.
4. **Generative AI Use:** Users should be aware of the ethical considerations and potential misuse of generative AI technologies, including the possibility of generating misleading or harmful content and/or plagiarism.
5. **Responsible Content Sharing:** Users should understand the importance of considering the validity and potential impact of information before sharing it online. This includes recognizing and not sharing "deepfake" content, or content generated or manipulated by AI to mislead or harm others. See Policy 320- Freedom of Speech and Political Activities.
6. **Cybersecurity Awareness:** Users should report any suspicious activity or perceived threats to the District's cybersecurity team using helpdesk@philasd.org.

Website Publisher Agreements

The District's Webmaster team within OITDM establishes the agreements for web publishers and sponsoring administrative superiors here.

Identified web publishers must complete a mandatory webinar, which includes content on website accessibility requirements, found here before being granted access to edit any District website.

School-based web publishers are assigned by their school administrator using Role Access Delegation.

Central Office-based web publishers must submit the web publisher authorization form found here in coordination with the Chief or cabinet-level executive that oversees the department or division website.

Wired and Wireless Internet Access

Staff and students are expected to connect to the District's internet on District-issued devices using their District-issued username and password.

The School District of Philadelphia does not provide any technical support for any individual (staff, student, guest, etc) who chooses to use a personal device on the District's internet network.

Access to the District's wired and wireless internet networks is governed by the following tenets:

1. **Secure Connections:** Users should only connect to secure, authorized District wireless networks or private, secure home networks used for remote work and avoid using public, unsecured networks when accessing sensitive data.
2. **Device Security:** Any District issued device connecting to the District's wireless network should have up-to-date antivirus software and operating systems to minimize security risks.
3. **Network Etiquette:** Users should respect network resources and not engage in activities that intentionally disrupt network performance or security, such as excessive downloading, streaming, or the use of unauthorized or illegal applications. The District controls web filtering and monitors network usage.
4. **Security Incidents:** If a user suspects that the security of their District-issued device or the wireless network has been compromised, they should report the incident immediately to helpdesk@philasd.org.
5. **Compliance with Policies:** Use of the wireless internet implies acceptance of and compliance with the District's security policies, procedures, and protocols as well as any applicable laws and regulations. See Policy 829 - Information Security for more information.
6. **Network Monitoring:** Users should be aware that the school district reserves the right to monitor network usage for the purpose of maintaining network security and performance.

Guest Access to the District's Wireless Network

Guest access to the District's wireless network must be sponsored by an existing active District staff member for:

- Individual Users
    - Maximum duration of access is 30 days

- An on-site event (such as a Back To School Night)
    - Maximum duration of access is 5 days

Information on sponsoring Guest Accounts can be found at https://www.philasd.org/ithelpdesk/nac/.

Digital Access Requests

Any District staff member may submit a request to block or unblock an internet resource (website, application, or extension) using the Digital Access Request application found in the Employee Portal (https://www.philasd.org/login).

In most cases, the school or department administrator must approve the filtering request prior to its review by the Office of Information Technology and Data Management. Submissions that identify ways staff or students are circumventing District security methods are directed immediately to the Information Security team for review.

Submissions are reviewed on a rolling basis.

Reporting Potential Policy Violations and/or Suspicious Activity

Protocols for reporting suspicious activities and/or conduct that violates this Policy:

1. **Identification:** Users should be alert for what constitutes suspicious activity or policy violation, such as phishing attempts, unauthorized system access, misuse of data, or inappropriate online behavior.
2. **Immediate Reporting:** Any suspicious activities or policy violations should be reported immediately to abuse@philasd.org to mitigate potential damage. Delays in reporting can escalate the impact of a security incident.
3. **Non-Retaliation:** There should be no retaliation for reporting suspicious activities or violations of the Acceptable Use Policy.
4. **Confidentiality:** Maintain the confidentiality of the reporter to the greatest extent possible under law and other Board Policies.

Maintenance Schedule

These Administrative Procedures will be reviewed upon review of the Policy, or upon a triggering event.