ADMINISTRATIVE PROCEDURE

INFORMATION TECHNOLOGY SERVICES
ACCEPTABLE USAGE

AP No. 0700
Effective Date: June 11, 2025

I. PURPOSE: To provide procedures instructing users to follow established practices in using technology in a responsible and productive manner.

II. POLICY:

The Prince George's County Board of Education (Board) is committed to providing a safe, productive, and equitable learning environment for all students, staff, and guests. The Prince George's County Public Schools (PGCPS) network infrastructure, including the Wide Area Network (WAN), Local Area Networks (LANs), Wi-Fi network, and cloud based networks, has been designed to support effective academic and business practice for the school system.

It is the expectation of the Board that all employees, students, and guests act in a responsible, civil, ethical, and appropriate manner when using PGCPS technology and digital tools. PGCPS reserves the right and has the express responsibility to monitor and filter network traffic to ensure compliance. (Policy 0115)

III. BACKGROUND: Prince George's County Public Schools (PGCPS) views technology (including computing devices, scanners, digital cameras, video projectors, printers, video cameras, and the Internet) as digital tools for learning, organizational efficiency, and effectiveness. PGCPS's network has been created to link school buildings, administrative sites, and support facilities together for the purposes of accessing and sharing information in accordance with the goals and objectives set forth. Any student who is a user of the PGCPS Network is expected to use technology resources for educational purposes only. As such, policies and procedures outlined in the Student Rights and Responsibilities Handbook apply to the use of all PGCPS technology tools. Employees, authorized contractors and volunteers of PGCPS are expected to use technology resources for educational and/or PGCPS administrative purposes only. Any

user of the PGCPS Network, Internet, and technologies should always reflect academic honesty, high ethical standards, and moral responsibility.

IV. DEFINITIONS:

A. *Account*– A user account that allows access to resources and services on a computer network, enabling users to authenticate and interact with network-based applications and data.

B. *Computing device* – Technology tools connecting to the PGCPS network.

C. *Cyberbullying* – The use of technology components by a user(s) to disseminate language (such as spreading rumors or gossip) or images that directly or indirectly abuses, alarms, annoys, embarrasses, harasses, harms, threatens or torments another or others.

D. *Local Accounts* – Refers to a user account that is created and managed on a single computer or device, granting access to resources and services available only on that specific machine, unlike domain accounts, which are managed centrally across a network.

E. *Personally Identifiable Information (PII)* – Any data that can be used to identify a specific individual, such as name, address, student or employee number or Social Security number, or other unique identifiers. The data may include information about a person's family, such as name, phone number or address, and alone or in combination, is linked or linkable to a specific individual and allows a person to be identified with reasonable certainty.

F. *PGCPS Network* – Refers to the interconnected computer systems and devices within the school district, allowing authorized users to share resources, communicate, and access the internet, often using a Local Area Network (LAN).

G. *Technology (Components)* – Refers to network infrastructure, school technology resources, personal devices, data, and information accessed and transmitted within the network.

H. *User* – Refers to PGCPS employees, permanent or temporary, substitutes, contractors and contractors' employees, vendors, and students enrolled in PGCPS who have access to the PGCPS network.

I. *VPN (Virtual Private Networking)* access – A connection to the PGCPS network, through a wired or wireless high-speed internet connection using VPN software.

V. PROCEDURES:

A. General Requirements

1. All users are responsible for the appropriate care and security of ALL PGCPS issued equipment/devices.

2. All users are responsible for any activity which occurs using their PGCPS user account.

3. All users are to log off all systems before they leave their workstation, whenever they walk away from their computer, and at the end of each workday.

4. All users are prohibited from sharing accounts and/or passwords with anyone. This includes logging into a machine so someone can use it.

5. No local accounts can be created on computers or mobile devices without prior approval from the Division of Information Technology (IT).

6. Only approved software may be installed on PGCPS devices. The approved software listing is located: https://www.pgcps.org/it. All software must be approved through the process defined in PGCPS Administrative Procedure 0707, *Procurement Installation and Development of Software.*

7. Personnel from the IT, school-based designees and staff authorized by the Chief Information Technology Officer are the only individuals who will have administrative rights to devices on the PGCPS domain.

8. No student or unauthorized user is to be given administrative rights and/or administrative passwords to any computer within the PGCPS domain.

9. Cyberbullying, where a user uses technology components to disseminate language (such as spreading rumors or gossip) or images that directly or indirectly abuses, alarms, annoys, embarrasses, harasses, harms, threatens or torments another or others, will not be tolerated.

10. All computers are to be joined to the PGCPS domain unless exempted by IT.

11. Student and/or employee information accessed by authorized users must be secured and reside on school system equipment or district approved online resources; access to information must be limited to authorized users only.

12. Students may only access information they are authorized to use and need for assignments and/or other school related activities.

13. Personally Identifiable Information (PII) must be stored securely and, if shared, by using data security tools approved by IT. All users are responsible for the

secure extraction and exchange of data if required by their school system duties. Users must not knowingly or unknowingly provide PII to unauthorized or unapproved recipients.

14. All users will be held accountable for any violations of the Board's Acceptable Usage policy, and this administrative procedure, that can be traced to their individual accounts.

15. Any security vulnerability (such as phishing or spam attack) identified by a user on technology that is a part of the PGCPS network must be immediately reported to PGCPS' IT service support desk by submitting an online ticket (http://help.pgcps.org/) or call (301-386-1549). Users must not open, download or demonstrate the vulnerability to anyone other than IT, including other users.

B. Technology Acceptable Uses

1. Acceptable use of technology and all related resources requires users to:

   a. Protect Personally Identifiable Information (PII);

   b. Refrain from using, sending, posting, or sharing negative, harmful, false, or hurtful content that may be considered embarrassing or humiliating, following the requirements in Board Policy 0115. This applies to public messages, private messages, email, and material posted on social media and Web pages;

   c. Respect all copyright laws, following the requirements in AP 6160;

   d. Respect network limitations when sending or receiving information. There is no limitation on the size of e-mails, either internally or externally. PGCPS does, however, have a 25Mb limit on attachments;

   e. Use devices for their intended educational and organizational purposes only; and

   f. Understand that use of the computing device or the network for illegal activities is strictly prohibited.

C. Prohibitions

1. The following actions are prohibited to all users of the PGCPS Network. They include, but are not limited to:

   a. Group account log-ins where individual user credentials are used outside the intended purpose and are shared by another or group of individuals;

b. Damaging computing devices, computer systems or computer networks, degrading or disrupting equipment of system performance;

c. Trespassing in another's files, folders or work;

d. Utilizing the network for commercial purposes;

e. Displaying a logo of any commercial entity not directly related to PGCPS;

f. Using a pgcps.org website for anything other than educational or administrative purposes as deemed appropriate by PGCPS. This includes having links to any external site that does not directly relate to the instructional and/or administrative goals of PGCPS;

g. Accessing or transmitting illegal or harmful content, including pornography, hate speech, violence, or gambling and materials that are libelous, slanderous, or defamatory accessing or linking to websites that contain material deemed vulgar or offensive. These include, but are not limited to, websites containing any text, graphic, audio or visual representation of sex, acts of perversion, or any vulgar or obscene material, or that contain images or representations of full frontal or partial nudity lacking in any educational, scientific, or artistic value. Except for educational purposes related to carrying out job responsibilities, users must avoid these websites and must under no circumstances, possess any of these materials on their computer;

h. Accessing or linking to websites that contain material deemed inappropriate. These include but are not limited to websites containing any text, graphic, audio or visual representation of materials that contradict a safe, productive, and inclusive learning and work environment. Except for educational purposes related to carrying out job responsibilities, all users are to avoid websites promoting hatred, racial/religious/sexual discrimination, use of illegal drugs/alcohol/tobacco, criminal activities and computer/network hacking;

i. Engaging in cyberbullying or harassment by using the PGCPS network or e-mail to promote the annoyance, harassment or attack of others;

j. Purporting to misrepresent PGCPS in any way whatsoever;

k. Utilizing the PGCPS network for any illegal activity, including violation of copyright or other licenses or contracts. Copyrighted material, including graphics, may not be displayed unless in compliance with Administrative Procedure 6160 or without specific written permission to do so;

l. Accessing social media or messaging sites that are not part of a class activity under direct supervision of a teacher or are educationally inappropriate; or are outside the scope of an employee's job responsibilities;

m. Using abusive or otherwise objectionable language in either public or private messages;

n. Posting anonymous messages;

o. Posting any files that prove detrimental to internet or network performance. This includes unauthorized scripts, programs, and large files that may impede network operations;

p. Engaging in activities that disrupt the network or compromise its security or may cause undue congestion of the network through large downloads of files, or by engaging in idle activities - *e.g.*, students playing games not part of a class activity, or employees involved in activities other than their job responsibilities;

q. Vandalizing the data of another user;

r. Attempting to gain unauthorized access to resources, files, or any device on the network; *e.g.*, use of hacking, spy ware tools, etc.;

s. Identifying oneself with another person's name, likeness or any misrepresentation of one's identity. This includes deep fakes and any video or digitally altered images of face or body used to misrepresent or falsely share information;

t. Using the username, password, or other credentials of another user;

u. The theft of data, equipment, or intellectual property;

v. Using school system technology and user credentials for personal or commercial gain; and

w. Engaging in any activity that is prohibited by school rules, Board policies and PGCPS administrative procedures.

D. Privacy and Electronic Surveillance

1. Users have no privacy expectations in the contents of their personal files and records of their online activity while using PGCPS technologies and the communications systems. All email, equipment, and documents created, composed, stored, transmitted, and/or received are and remain at all times the

property of PGCPS. These items are not the private property of any employee or individual, and no employee or individual should have any expectation of privacy when using PGCPS communications systems. PGCPS may conduct monitoring and auditing activities from time to time to verify user compliance with the policy and administrative procedure.

2. PGCPS specifically reserves the right to access electronic communications and computer files at any time, including but not limited to, whenever necessary for corporate investigations into allegations of misconduct, fraud, or other wrongdoing, for technical maintenance purposes, to assure system security and compliance with Board policy or applicable legal requirements, and any other business purpose.

E. Consequences

1. If it has been determined that a user has improperly used equipment, the network, or PGCPS technology resources in any manner, the user can expect disciplinary action(s) which may include, but are not limited to:

   a. Immediate suspension of access to equipment and/or account(s);

   b. Disciplinary action by school/office administration; and

   c. Arrest and prosecution.

F. Web Acceptable Uses

1. Acceptable use of PGCPS Websites and all related resources requires web managers to:

   a. Use the website to improve communications and services of the school or office with students, staff, parents and the entire PGCPS community;

   b. Protect Personally Identifiable Information (PII) – PGCPS employees must not disclose on the Internet or on school district websites or web pages any PII concerning students (including without limitation names, addresses, or photographs) who have elected to opt-out of such publication through the district's opt-out process;

   c. Use appropriate language;

   d. Respect all copyright laws. Copyrighted material, including graphics, may not be displayed unless in compliance with Administrative Procedure 6160 or without specific written permission to do so;

e. Use the issued web account for the intended educational and administrative purposes only;

f. Understand that use of the website for illegal activities is strictly prohibited;

g. Identify a specific person by first and last name and ensure written permission is acquired by way of the standard PGCPS release if using a photograph or video on a web page.

h. Never utilize the network for commercial purposes.

G. Process for Reporting Inappropriate Use of the Network or Website

1. If a user believes that there has been a violation of these guidelines, the user is to immediately contact a teacher, school administrator or supervisor. A good rule of thumb is, "when in doubt … ask."

2. Employees may also submit an online help desk ticket (http://help.pgcps.org/) for support, and in urgent matters, can call the IT service help desk phone line at (301-386-1549).

H. E-mail Services

1. Every PGCPS user is eligible for an email account.

2. Users must:

a. Use their PGCPS email address for school system business only; and

b. Be advised to acquire and use their personal (non-PGCPS) e-mail address when signing up for distribution lists, circulars, newsletters, or any other non-educational and/or personal information.

I. Mobile Devices

1. PGCPS provides devices to designated employees which must be used for the sole purpose of conducting official school system business. Any personal use charges associated with the device are the responsibility of the individual user.

2. Replacement of all lost, stolen or damaged devices and/or accessories will be the responsibility of the user.

J. Virtual Private Network (VPN) Access

IT currently grants VPN access to authorized users in order to access the PGCPS network resources from an external location. This is detailed in Administrative Procedure 0705 – Information Technology Services Remote Access Procedures.

VI. MONITORING AND COMPLIANCE:

A. Authorized staff in IT will actively scan devices connected to the PGCPS network to ensure compliance with this administrative procedure. Scanning may take place remotely or physically by technical support staff. Installed software identified as being out of compliance with this administrative procedure will be uninstalled/removed from the device.

B. Best efforts will be made to contact the responsible user to verify compliance prior to the removal of the software. However, if the user cannot be contacted within a reasonable time, the software will be removed without further attempts to notify user(s).

VII. RELATED ADMINISTRATIVE PROCEDURES:

Administrative Procedure 0701 – Information Technology Services Google Workspace Procedures
Administrative Procedure 6160 – Copyright Guidelines
Administrative Procedure 10101 – Student Rights and Responsibilities Handbook

VIII. LEGAL REFERENCES:

- Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501-6505
- Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2523
- Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232(g)
- Student Data Privacy Act of 2015, MD. CODE ANN., EDUC. § 4-131
- Username and Password Privacy Protection and Exclusions, MD. CODE ANN., LAB. AND EMP. § 3-712

IX. MAINTENANCE AND UPDATE OF THIS ADMINISTRATIVE PROCEDURE:

This administrative procedure originates with the Division of Information Technology and will be updated, as needed.

X. CANCELLATIONS AND SUPERSEDURES:

This administrative procedure cancels and supersedes Administrative Procedure 0700 dated July 1, 2019.

XI. EFFECTIVE DATE: June 11, 2025