ADMINISTRATIVE PROCEDURE

INFORMATION TECHNOLOGY SERVICES
GOOGLE WORKSPACE PROCEDURES

AP 0701
Effective Date:
September 1, 2025

I. **PURPOSE:** To provide Google Workspace procedures for users of Prince George's County Public Schools (PGCPS) technology resources.

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:** Every PGCPS student and employee receives an email account automatically. Accounts for non-employees may be obtained with the approval of a PGCPS supervisor. All email accounts and the information contained within are the property of PGCPS and, as such, can be reviewed at any time. There is no expectation of privacy in PGCPS email accounts.

Authorized Users 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. Authorized Users must abide by email procedures as set forth in this administrative procedure. PGCPS uses "Google Workspace for Education," a suite of hosted email and collaboration applications exclusively for schools and universities.

IV. DEFINITIONS:

A. *Authorized User* – A student, employee, student teacher, volunteer, contractor, or any other entity or individual provided an email account with PGCPS.

B. *Distribution Group* – The process by which emails can be sent to a group of users without the need to enter each recipient's individual address in the "to field."

C. Email Records – The combination of emails drafted, sent, received, and archived by a user, including any attachments, and messages shared through google chat

D. *Generic Accounts* – An individual user account (or shared account by Identified individuals) based on the user(s) role, function or office that is used to appropriately respond and handle (i.e. hr.recruitment@pgcps.org and communications@pgcps.org)

E. *Google Drive* – A cloud-based storage service that allows users to store, access, and sync files across multiple devices. It also provides access to web-based applications for creating documents, spreadsheets, and presentations in a secure environment.

F. *Google Site* – A web-based tool that allows users to create and publish websites without needing to learn design or programming: As a part of a Google Workspace, it includes real-time co-editing and sharing, easy access to content from Google

G. *Google Workspace* – A collection of cloud-based tools that help users and organizations collaborate and increase productivity, in a secured environment.

H *Inbound email* – Email(s) sent from external networks into the PGCPS network.

I. *Internal email* – Email(s) sent between users of the PGCPS email system.

J. *Mass Mailings* – The act of sending the same message to a large group of people at the same time.

K. *Multi-Factor authentication* – A security process that requires more than one form of identification for logon (password and verification code) of an authorized user to reduce the chance of account information being stolen or compromised. *Multi-Factor authentication* can include a notification on a phone, rotating numeric token, or other methods as needed to obtain and maintain secure access.

L. *Outbound email* – Email(s) sent from the PGCPS network to external networks.

M. *PGCPS Sponsor* – PGCPS supervisor who supports and is responsible for the access and activities on the network and google workspace.

N. *Phishing Emails* – The practice of sending fraudulent communications that appear to come from a legitimate and reputable source, usually through email and text messaging

O. *Security Group* –A group of users who have been provisioned specific access to PGCPS network resources (i.e. document, server, platform, etc.) to perform their school or work duties based on their identified position number and classification, to ensure security of resources.

P. *SPAM* – Internal or external unsolicited or bulk email.

V. PROCEDURES:

A. Email Access for Employee Users

1. All employees receive Windows, Oracle E-Business, and email accounts within 24 hours of the start date entered in Oracle by Human Resources.

2. Employees have unlimited access to their email accounts via the Internet from either inside or outside the PGCPS network. Access to email from inside or outside of the network requires Multi-Factor Verification.

3. PGCPS does not welcome or permit SPAM and other solicitations. PGCPS Information Technology Staff will make every effort to reduce or eliminate SPAM by ensuring each piece of incoming and outgoing email is scanned, and by screening and eliminating unsolicited email and email with no primary addressee that uses "blind copy" distribution to reach employees., is impossible to prevent all SPAM from entering the email system, all users must remain vigilant in their efforts to reduce SPAM by appropriately using their accounts only for school and business purposes.

   Additionally, for network security reasons, PGCPS will not permit the release of mass mailing list of user addresses that could be used to launch phishing campaigns and any other unsolicited bulk email aimed at PGCPS users.

4. PGCPS will review and prohibit mass mailings to staff members by either internal or external sources. Internal mass mailings must receive approval from the Superintendent or Chief Information Technology Officer.

5. Each Inbound, outbound, and internal email and attachment is limited to 25Mb (megabytes).

6. Antivirus procedures may strip or prohibit certain attachment file types. Zipped files (".zip") where multiple files are combined and compressed into one file, and executable files (".exe."), essentially files that contain programs for running software, are the most notable prohibited types. The Information Technology (IT) Division reserves the authority to block any file type deemed by PGCPS's virus protection software as being harmful or potentially harmful.

7. All users will have at least 10 GB (gigabytes) of storage space for their mail, calendar, contacts, chats, photos, and documents.

8. Email records for all employees will be maintained and accessed by PGCPS for at least one year.

9. All email sent or received using PGCPS systems is the property of PGCPS. As such, PGCPS has the right to review email at any time, without notice.

10. User locations are assigned by Human Resources based on position codes. The user's account is automatically placed into their primary assigned school or department staff group designated in Oracle by Information Technology staff based Human Resource's determination. This membership is used for the application of group policies and security permissions and also ensure the user will receive emails directed to all staff members.

11. All access to PGCPS IT systems, including, but not limited to, Google Workspace, is automatically removed at midnight on the date of separation. This includes both voluntary and involuntary termination and retirement. It is important for employees and supervisors to develop transition plans, when possible, that also include the sharing of resources (emails, documents, etc.) in the Google environment.

B. Email Access for Non-employees

1. Accounts for non-employees are created on an as needed basis and fall into one of three (3) categories:

    a. Generic accounts: accounts for ease of email distribution or for specific programs and services, not linked to any one user;

    b. Contractor accounts: accounts for internal users who access the PGCPS network and IT systems; and

c. Non-PGCPS employee accounts (e.g. student teachers, speech pathologists, etc.): accounts for internal users who are not paid directly through PGCPS payroll and do not have an employee identification number (EIN).

2. All Generic, Contractor, and Non-PGCPS employee accounts must adhere to the same standards as all PGCPS employee email accounts. For more information on these rules, please see Administrative Procedure 0700, Information Technology Services-Acceptable Usage Guidelines.

3. Generic accounts

   a. To request a generic account, complete the form entitled "*Generic Account Request Form"* located at http://eforms.pgcps.org/ from within the PGCPS network.

   b. Information Technology staff will create these accounts within three (3) business days of receipt of the form and the logon information will be sent directly to the requestor.

   c. Generic accounts are configured to log into PGCPS email, but not for logging into PGCPS devices. PGCPS does not allow any staff or student to log onto PGCPS computers anonymously, which could be the case if a generic account worked for PGCPS devices. They are only to be used for the specific purpose for which they were requested.

4. Contractor accounts

   a. To request a contractor account, the PGCPS sponsor should complete the form entitled *"Windows & Remote Access Form for Contractors"* located at http://eforms.pgcps.org/.

   b. When the account is requested, an end-date must be given. This end-date must occur on or before July 1 of the current school year.

   c. These accounts are created within three (3) business days of the completion of the form and the logon information will be sent directly to the PGCPS sponsor.

   d. These accounts must be renewed each school year, if needed.

5. Non-PGCPS employee accounts

a. To request a non-PGCPS employee account, the PGCPS sponsor should complete the form entitled, *Non-PGCPS Employee Request Form* located at http://eforms.pgcps.org.

b. When the account is requested, an end-date must be given. This end- date must occur on or before July 1 of the current school year.

c. These accounts are created within three (3) business days of the completion of the form and the logon information will be sent directly to the PGCP sponsor.

d. These accounts must be renewed each school year, if needed.

6. Parent Teacher organizations and volunteers are not eligible for Windows logons or email accounts.

C. Email Access for Students

1. All students receive accounts within 24 hours of their enrollment start date.

2. Students have unlimited access to their mailbox from inside or outside the PGCPS network.

3. All students have at least 2 GB of storage for their email and documents.

4. Student accounts may only send and receive email internally for the security of our students and establishing a safe learning environment. Occasionally, exceptions are made for external email addresses the specific case and academic purpose can be shared in a HELP desk ticket from a teacher or school administrator. A past example is high school students needing to receive emails from the College Board.

5. Student accounts are automatically placed into their school's distribution group. All email messages sent to school student groups are moderated by identified school-based administrator or designee.

6. All email sent or received using PGCPS systems is the property of PGCPS. As such, PGCPS has the right to review email at any time, without notice.

D. User Responsibilities

1. Users are required to use their PGCPS email address for all school system business. Users are advised to acquire and use a personal email address for all other email correspondence.

2. Users must never use their PGCPS email address for personal or financial gain. This includes sending emails to PGCPS staff or students that are unsolicited and will provide personal or financial gain for individuals. In accordance with Administrative Procedure 0700 -Information Technology Services - Acceptable Usage Guidelines, users must never use their PGCPS email address to annoy, harass or solicit other PGCPS staff members, students, or external email users. Employees found violating these guidelines may be subject to disciplinary action.

3. In alignment with the annual Safe School training for PGCPS, all users should make every attempt to avoid clicking on phishing emails or scams. Additionally, PGCPS Information Technology staff will routinely run simulated phishing campaigns and provide appropriate resources for any user who may require a refresher.

4. Email display names should state the employee's legal first and last name. Users should not change their display names to show any name that does not identify their name properly to the reader.

5. Email is to be used in a professional manner, void of foul, abusive or threatening language, and/or language that is of indecent nature or content.

6. All employees must place a signature at the bottom of each email sent which should only include:

    a. Employee's Name (bold type) Preferred Pronoun* (italic);

    b. Employee's Title (italic type);

    c. Employee's School or Department;

    d. Prince George's County Public Schools;

    e. Employee's Office Telephone Number | Employee's Cell Phone Number | PGCPS Social Media Info;

    f. Email address; and

    g. No quotations or other slogans should be used. Instructions for creating and modifying signatures can be found at: https://support.google.com/mail/answer/8395?hl=en&co=GENIE.Platform%3DDesktop.

7. If an employee is unavailable for an extended period of time an Out-of-Office message, or Vacation Responder should be placed on their mailbox for the days

they will be unavailable. This message should also include instructions for alternate assistance, if available. Employees should not leave Out-of-Office messages on their mailbox indefinitely and should ensure that the message is removed upon their return to work. Instructions for creating and modifying these messages can be found at: https://support.google.com/mail/answer/25922?hl=en&ref_topic=3394219&sjid=2135189259102345055-NA.

E. Email Etiquette

1. All users of the PGCPS email system should follow the following guidelines when communicating.

   a. Always limit communication to educational or PGCPS business purposes only.

   b. Always be professional in all Email communication.

   c. Use the subject line to identify the subject of the message and do not leave it blank.

   d. Use proper grammar, punctuation, and spelling.

   e. Do not attach unnecessary files, especially those that exceed the limit of 25 MB.

   f. Do not write in CAPITALS.

   g. Employee users should always sign emails with a professional signature, typically including full name, job title, department or division, Prince George's County Public County School and contact information. Signatures should be concise and use common closing phrases include "Sincerely," "Regards," "Best regards," or "Thank you.

   h. Do not initiate or forward SPAM and unsolicited mass mailings.

   i. Do not use email to discuss confidential information with staff or other individuals who do not have legitimate educational interest or authority to review the information.

   j. Do not configure your PGCPS email account to automatically forward to your personal account or other external accounts.

k. Do not send or forward emails containing libelous, defamatory, offensive, racist, or obscene remarks.

l. Keep in mind that electronic communication does not convey facial expressions or tone of voice. It is important to be aware of how the message written could be interpreted and/or misunderstood.

m. When sending a mass mailing, the sender should use the blind carbon copy (BCC) field so that you do not wrongfully publish another person's email address to others. When using the BCC field, the recipient will receive a copy of the email, but their address will be hidden from all other recipients of the message.

n. Do not include attachments that contain Personal Identifiable Information (PII) of students, parents or staff members.

2. In addition to the guidelines listed above, those employees communicating with students should also follow the following guidelines.

   a. Hold yourself to the same standards of written communication to which students are held.

   b. Contact with students should be limited to educational or school-related purposes only and follow the employee code of conduct expectations of Conduct with Students.

   c. Always address the student properly and sign the message with your professional name.

   d. Do not include attachments that contain Personal Identifiable Information (PII) of students, parents or staff members.

3. In addition to the guidelines listed above, those employees communicating with parents and other members of the community should also follow these guidelines.

   a. Hold yourself to professional standards of written communication and use proper grammar, punctuation and spelling.

   b. Answer all emails within 48 hours, Parents and community members send an email because they wish to receive a quick response. If you do not have the time to respond properly, send a reply acknowledging the sender's email and follow up with another response when you have more time or as soon as more information is available.

F. Google Chat Acceptable Uses

1. Google Chat is an instant messaging product available to all PGCPS employees. It is useful for speaking with colleagues in a timely and simple manner.

2. Google Chat should be used for business/educational purposes only.

3. It should not be used to harass, annoy, or cause harm to any individuals.

4. When using Google Chat, do not give out any student or staff information.

5. Employees are not required to use Google Chat or to accept invitations to chat with others.

G. Google Sites Acceptable Uses

1. Google Sites are provided as an online tool in support of a collaborative work effort at PGCPS. Their use is, therefore, restricted to PGCPS-affiliated groups, departments and organizations only. Google Sites should not be created for personal use that is outside the scope of academic or professional responsibilities.

   Google sites must adhere to all federal, state and local laws, policies, regulations, and procedures for employees of PGCPS and adhere to all information technology use guidelines in Administrative Procedure 0700.

2. Google Sites allow any employee to create an internal or external webpage for centralized access to information. The best use of Google Sites is for internal departmental collaboration and information sharing. In the school environment, Google Sites can be a great way to provide information to students and parents on assignments, upcoming events, and access to permission forms or other documents.

3. Use of Google Sites must be consistent with the educational goals and mission of PGCPS, as well as comply with local, state and federal laws and regulations, including but not limited to, copyright and trademark law. Google Sites must adhere to PGCPS policies and administrative procedures.

4. It will be the Google Site creator's responsibility to maintain the Site and ensure that all information contained therein is accurate, up-to-date, and is in conformance with the mission and values of PGCPS.

5. PGCPS IT staff reserves the right to immediately remove any Google Site that they find to be in violation of any portion of this administrative procedure with or without prior notice to the Site owner.

6. No confidential information may be contained in a Google Site. This includes, but is not limited to:

    a. Social Security Numbers;

    b. Employee Information Numbers (EIN);

    c. Student educational records;

    d. Student or employee medical records;

    e. Employee or student specific financial data; and

    f. Birth Date.

7. Users are expected to report misuse of a Google Site to IT staff as soon as possible so that a proper course of action can be determined in a timely fashion.

8. Google Sites should not be used to create departmental, divisional sites, or official school sites. These sites should be created in with approved tools and resources provided by the PGCPS Web Services Team.

9. Proper security measures, such as providing access to view or edit to specific individuals within PGCPS, should be taken to secure the Google Site, accordingly.

10. Employees cannot use Google Sites to promote any personal business or entity for financial gain or notoriety.

11. Upon termination or separation of employment, all access to Google Sites is automatically removed by the end of the business day. This automation is determined by the separation date provided by Human Resources in Oracle E-Business Suite.

H. Google Drive Acceptable Use

1. Google Drive provides all PGCPS employees with online access to create documents, spreadsheets, and presentation editing and storage.

2. When storing files in Google Drive, users should always limit access and secure documents by only providing access specific individuals to view or edit documents. This ensures that information is protected and appropriately used for its intended purpose.

3. All files stored should be professional in nature and limited to business or educational purposes. No personal documents should be stored in Google Drive under your pgcps.org account.

4. Upon termination or separation of employment, all access to Google Drive is automatically removed by the end of the business day. This automation is determined by the separation date provided by Human Resources in Oracle E-Business Suite.

I. Termination of Employment

1. By the close of business of the date of separation, the employee's account is disabled. This automation is determined by the separation date provided by Human Resources in Oracle E-Business Suite.

2. Once employment is terminated and the employee's account is disabled, no access will be granted to the employee unless requested in writing from the Chief Information Technology Officer.

3. Prior to termination, employees must transfer access of any files needed by their office for business continuity.

J. Security and Distribution Groups

1. Security Groups:

   a. Are used mainly for controlling access to one or more programs, services, or resources, such as files, folders, or shares;

   b. Can be composed of users, computers, or subgroups;

   c. Can also have email capability, if required; and

   d. Are usually maintained by the Division of Information Technology.

   e. To request this type of group, please complete the form entitled, *"Security, Distribution and Google Groups Request"* at http://eforms.pgcps.org.

2. Distribution Groups:

   a. Are used solely for distribution of email to a cluster of users;

   b. Generally used to provide global access to distribution lists; and

c. Maintained by IT Staff.

d. To request this type of group, please complete the form entitled, *"Security, Distribution and Google Groups Request"* at *http://eforms.pgcps.org*

VI. MONITORING AND COMPLIANCE:

A. Authorized staff in the Division of Information Technology will manage access to mail and Google Apps and requests for mail access for non-employees, security and distribution groups in accordance with this Procedure.

B. Staff should promptly report potential misuse of a Google Site to the Division of Information Technology for investigation and prompt resolution.

VII. RELATED ADMINISTRATIVE PROCEDURES:

Administrative Procedure 0700 – Information Technology Services – Acceptable Usage Guidelines

VIII. MAINTENANCE AND UPDATE OF THIS ADMINISTRATIVE PROCEDURE:

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

IX. CANCELLATIONS AND SUPERSEDURES: This administrative procedure cancels and supersedes Administrative Procedure 0701, dated July 1, 2019.

X. EFFECTIVE DATE: September 1, 2025

Distribution: Lists 1, 2, 3, 4, 5, 8, 9 and 10