Plainfield Public School District
Information Technology Department
Standard Operating Procedures

Responsibility and Goal of the IT Department

The Office of Information Technology provides the Plainfield Public School District's students and staff with the infrastructure, systems, and support of efficient technology for student achievement and to build staff capacity for teaching and learning.
As Technology plays a vital role in education today, the goal of the IT Department is to improve the quality of education for students and teachers by providing reliable information technology systems to students, faculty, staff and parents as they employ technology in the K-12 learning process.

Contact Information

Information Technology Center:	1800 West Front Street, Plainfield NJ 07060 (908) 731-4365
Helpdesk Support/Call Center:	helpdesk@plainfield.k12.nj.us (908) 731-4200 ext.: 5555
Supervisor of Information Technology : (Technical Operations)	Destiny Simons dsimons@plainfield.k12.nj.us (908) 731-4200 ext.: 5345
Supervisor of Information Technology : (Network Infrastructures)	Gary Bloom gbloom@plainfield.k12.nj.us (908) 731-4444
Chief Information Technology Officer:	Christopher Payne cpayne@plainfield.k12.nj.us (908) 731-4363

What We Support

Hardware

Staff will be provided with all necessary technology hardware devices the district may deem necessary for your position. Only District approved assets are allowed on premises and connected to the Plainfield Public Schools wide area network. Any attempt to do otherwise is a violation of the District Acceptable Use Policy (See attached) and subject to disciplinary action. If additional hardware is required, a hardware request form must be completed and submitted by your appropriate department head or supervisor. ***(see Form IT-HPR001, p.7)***

Software and Applications

Only district approved software should be installed on your work devices. All other software and applications will be removed. If additional software or applications are required, a software request form must be completed and submitted by your department head or supervisor. ***(see Form IT-SAR002, p.7)***

Telephones/Communications

Communication devices will be provided when appropriate or necessary for staff use.

District Phone system (VOIP)

The district will provide desk phones and support to staff when needed. If additional phones or extensions are needed, the appropriate Telco Form must be completed and submitted once approved by administration. ***(see Form IT-TSW003, p.7)***

Cellular Devices

The district will provide cellular devices and support to staff when needed. All requests for cell phones require the approval of the department head only. ***(see Form IT-TDCE004, p.7)***

District cell phone numbers will be published and are governed by the acceptable use policy and should be used appropriately. All device use can be monitored by the School District when needed. The Department strongly advises that the device should be used for school business only.

User Accounts, Email and Passwords

User Account and Authentication

Usernames and Passwords: Each end user will be provided with a unique username and temporary password. Users must, when prompted, access various IT systems and services. Users are expected to keep passwords confidential. The IT department will force users to change them periodically. Passwords must adhere to industry complexity standards.

Passwords must be 8 characters or more in length with the following requirements:

1. No usernames or display name
2. No sequences of more than 4 digits in a row
3. Include at least one character from three (3) of these categories:
    - Uppercase letter

- Lowercase letter
- Number
- Special character (! $ %)

Multi-Factor Authentication (MFA): User accounts with a higher level of clearance and access will be required to add an extra layer of security to your accounts. This service (feature) will be provided by the IT department if necessary.

Email Usage

Email Account: Use the organization's official email account for all work-related communication.

Email Etiquette: Follow professional email etiquette, use clear subject lines, and avoid sending sensitive information via email.

Phishing Awareness: Be cautious of phishing attempts and report suspicious emails to the IT department via the IT support desk or administration.

Internet Access

The IT Department provides all internet access for staff and students throughout the school district. This access is monitored through our filtration software to prevent access to sites which are inappropriate, illegal or against PPSD policy.

Wireless Networks

Any device utilizing access to the network infrastructure is subject to the following:

1. All use of wireless access points and devices must comply with district policies for Acceptable Use.
2. Only managed, district-owned wireless access points may be attached to the district network.
3. Only managed, district-owned devices are supported by the district's wireless network.
4. Any wireless access point or device must utilize IP address space as assigned by network management via a static or dynamic address assignment.

Remote Access

When deemed necessary, users may be provided with the ability to work remotely. If this is needed, please contact the IT Support desk for assistance.

Relocation of Computers or Printers

All district stationery technology equipment (Desktop computers, Printers, Copiers, TVs, Smart displays) should only be moved or relocated by the appropriate staff. Request for assistance must be submitted via the appropriate IT move form, when requesting moves we ask that you be mindful of the noted 5 Business days timeline. ***(see Form IT-TER005, p.7)***

Data Backup

The IT Department provides complete automatic backup services of user data, if stored appropriately *(See file storage)*

Saving files and Storage of data

File Storage: please save files on your district provided network drives or cloud storage (One Drive) provided by the organization for data backup and accessibility.

Security

Security Best Practices

Data Protection: Handle sensitive data responsibly and in compliance with the organization's data protection policies.

Screen Locking: Lock your computer when not in use to prevent unauthorized access.

Social Engineering Awareness: Be cautious of social engineering attempts and avoid sharing sensitive information with unknown individuals.

Support Request

How to Request IT Support as an End User

If you encounter technical issues or need assistance with IT-related matters, follow these steps to request support from the IT department:

1. Contact the Help Desk/Call Center:

The first step is to reach out to the IT help desk/call center, which is the primary point of contact for IT support requests. *(See Contact Information)*

2. Provide Detailed Information:

When submitting your support request, provide detailed information about the issue you are facing. Include any error messages, specific symptoms, or steps to reproduce the problem.

3. Include Relevant Details:

Include your full name, department, building or school, room number, asset tag when appropriate, and contact information in the support request to ensure the IT team can reach you if needed.

4. Prioritize Urgency:

If the issue is urgent and impacting your work or business operations, clearly indicate the urgency in your support request.

6. Follow-Up Information:

Be available to provide additional information or respond to inquiries from the IT support team if they require further details to resolve the issue.

7. Use Self-Help Resources (Optional):

If applicable, check the organization's knowledge base, FAQs, or user guides for self-help solutions before requesting support. You might find the answer to your problem there and resolve the issue without waiting for assistance.

8. Be Patient:

After submitting your support request, be patient and allow the IT support team some time to investigate and address the issue. Please do not attempt to open an additional support request, as this may only further delay and confuse the resolution of your issue.

9. Ticket Updates:

Keep an eye on updates to your support ticket. The IT team may provide status updates or additional questions through the ticketing system or email.

10. Follow Up (if Necessary):

If you have not received a response or resolution within a reasonable time frame, consider following up on your support request with a polite reminder.

11. Feedback and Confirmation:

Once the issue is resolved, provide feedback on your support experience, either through a post-interaction survey or by directly reaching out to the IT department. Confirm that the issue has been resolved to your satisfaction.

Remember, clear communication and providing accurate information are essential to receiving efficient and effective IT support. The IT department is there to help you, so don't hesitate to seek assistance when needed.

12. Travel outside the US:

Our network is secured by the best practices in keeping our network safe. When traveling outside the United States, you must get approval from the Department Head***. (see Form IT-TOC006, p.7)***

Districtwide/School In-Person and Virtual Events

In collaboration with the Office of Information Technology, the Office of Marketing and Communications schedules, sets up, hosts, and streams in-person, hybrid, and virtual events (meetings, town halls, events, etc.) via Zoom and other streaming platforms.

The initial meeting(s) should occur at least one month prior to the event to establish technical support, participants, presentation, supporting media, and needs from the Office of Marketing and Communications.

If the schedule does not allow for direct support of a live event, best efforts will be made to ensure the asking department/school is provided with the resources to host the event.

Digital Signage/Electronic Marquees (Indoor + Outdoor)

In collaboration with the Office of Information Technology, the Office of Marketing and Communications will provide content and oversight of all digital signage (electronic outdoor marquees and indoor electronic marquees/signage) located in all school buildings and offices.
For training or a content request, all employees must contact the Office of Marketing and Communications at, (908) 731-4442 or by email at, information@plainfield.k12.nj.us.

References

1.Telephones

Avaya 9608 Quick Reference Guide

Avaya J129 Quick Reference Guide

Avaya J179 Quick Reference Guide

2. Acceptable Use Policy (AUP)

Internet Safety and Technology
Policy Manual: Code 6142.10
http://go.boarddocs.com/nj/plainfield/Board.nsf/goto?open&id=BG3JSH4DD0F9

Forms

1. (***Hardware form # IT-HPR001***)

Hardware Approval Request IT-HPR001

2. ***(Software form # IT-SAR002)***

Software Approval Request IT-SAR002

3. ***(Telco form # IT-TSW003)***

Telco Service Wiring IT-TSW003

4. (***Mobile device form # IT-TDCE004***)

Cell Phone Request Form IT-TDCE004

5. ***(Relocation form # IT-TER005)***

Tech Relocation IT-TER005

6. (***Travel form # IT-TOC006)***

Travel Outside the US Approval Request (District Equipment) IT-TOC006

FAQs

How do I log in to my work computer or access the school's network?

a. You can log in to your work computer using your assigned credentials (username and password). If you encounter any login issues, contact the IT helpdesk/call center for assistance. To contact the Help Desk/Call Center you can dial ext. 5555 from any district phone or send an email to helpdesk@plainfield.k12.nj.us

1. **How can I access my email account and reset my email password?**
   a. You can access your email through the school's webmail portal or an email client, Outlook. If you need to reset your email password, follow the password reset procedure outlined in the IT Department SOP or contact the IT helpdesk/call center.

2. **What should I do if I forget my login password for the school's systems?**
   a. If you forget your password, contact the IT helpdesk/call center immediately to initiate a password reset process.

3. **Can I connect personal devices to the school's network or Wi-Fi?**
   a. The school's network is primarily for work-related devices. Please refrain from connecting personal devices, such as Google Home, Alexa Devices, and other personal devices, unless explicitly permitted by the IT Department and follow the acceptable use policy.

4. **How can I request technical support for IT issues or equipment malfunctions?**
   a. To request technical support, submit a ticket through the designated helpdesk/call center system or contact the IT helpdesk/call center via phone or email. Be sure to provide a detailed description of the issue for a prompt resolution.

5. **Is there a policy for software and application installations on work computers?**
   a. Work computers are typically managed by the IT Department. Please refrain from installing unauthorized software. If you require specific software, a software request form must be filled out and submitted to the IT Department. Once we receive your request, we will begin our evaluation and installation of the software.

6. **What cybersecurity measures should I be aware of while using school devices or networks?**
   a. Be cautious with emails from unknown sources, avoid clicking on suspicious links or attachments, and report any security concerns immediately to the IT Department. Follow the acceptable use policy to ensure the security of our systems.

7. **How often do I need to update my password?**
   a. Password update frequency may vary, but as a general rule, change your password every 90 days or as mandated by the school's IT security policy.

8. **What is the procedure for requesting new IT equipment or accessories?**

a. To request new IT equipment or accessories, submit a purchase request following the guidelines in the IT Department SOP. Include the necessary details and obtain the required approvals before proceeding with the purchase.

9. **How can I access training resources to enhance my technology skills?**
   a. The school may provide access to training resources or workshops for staff. Inquire with your supervisor or the HR department about available opportunities.

10. **What do I do in case of a data breach or data loss incident?**
    a. If you suspect a data breach or data loss, immediately report the incident to the IT Department and follow the established incident reporting procedures.

11. **Can I use my work email for personal communications?**
    a. It is recommended to use your work email strictly for work-related communications. Avoid using it for personal purposes to maintain a secure and professional environment.

12. **Can I access my work email from outside the United States?**
    a. Our network is secured by best practice. We can allow access, but there are restrictions. Please fill out the travel equipment form. Be sure to provide the following information on the phone: name, country location, and dates of travel.

13. **Can I use my district cell phone outside of the United States?**
    a. Our network and equipment are secured by best practice, thus not allowing out-of-county access to our infrastructure. Do not bring/use your district cell phone outside of the district without filling out the appropriate form and getting a signature from your department head.

14. **Are there any guidelines for data storage and file organization?**
    a. The Plainfield Public School District utilizes a cloud storage solution called OneDrive. OneDrive lets you store and protect your files, share them with others, and get to them from anywhere on all your devices (internet connectivity required). The IT Department SOP may include guidelines for data storage, file organization, and proper backup procedures. Adhering to these guidelines will help maintain data integrity and security.

15. **How are software updates and patches managed on our work devices?**
    a. Software updates and patches are typically managed centrally by the IT Department. The updates are scheduled and rolled out to ensure the devices are up to date and secure.

16. **Where can I find information about the school's technology policies and procedures?**
    a. You can access the school's technology policies and procedures in the IT Department SOP, which is usually available on the school's intranet or shared document repository.

17. **What is Social Engineering Awareness?**
    a. Social engineering is the act of exploiting human weaknesses to gain access to personal information and protected systems. Social engineering relies on manipulating individuals rather

than hacking computer systems to penetrate a target's account. Some common examples of Social Engineering are:

- Phishing attempts
- Spear phishing
- Quid Pro Quo attacks (i.e., tech support scams)
- Scareware

For more information on these attempts please see the glossary.

Glossary of Terms

Antivirus Software – Programs designed to detect, prevent, and remove malicious software (malware) from computers or devices.

Backup - A copy of important data and files created to protect against data loss due to hardware failure, accidental deletion, or other issues.

Browser – Software used to access and view websites on the internet. Common examples include Google Chrome, Mozilla Firefox, Microsoft Edge, or Safari.

Cloud Storage - Online storage services that allow users to store and access data and files over the internet, such as Google Drive and OneDrive.

Device – A device that processes data and performs various tasks using software programs. When the word “device” is used it could reference a computer or a mobile device such as a laptop, Chromebook, phone, or iPad.

Firewall- A security system that protects a computer network from unauthorized access and potential threats.

Hardware/Accessories - The physical components of a computer or device, such as the monitor, keyboard, mouse, and CPU.

Login - The process of entering a username and password to access a computer, network, or online account.

Logout - The process of ending a session and logging out of a computer or account to protect privacy and security.

Phishing - A fraudulent attempt to obtain sensitive information, such as usernames, passwords, or credit card details, by disguising as a trustworthy entity.

Quid pro quo attack – A type of social engineering cyberattack where an attacker offers something in exchange for sensitive information or access to a victim's computer or network. During a quid pro quo attack, the attacker typically contacts the victim, posing as a helpful individual, service provider, or technical support personnel. They might claim to be from a reputable company or a trusted organization and offer assistance or rewards to gain the victim's trust.

Scareware - A type of malicious software or deceptive tactic used by cybercriminals to scare and trick people into taking certain actions. This tactic aims to create fear or anxiety in the victim, pushing them to believe that their computer is infected with a dangerous virus or facing a critical security issue.

Social Engineering - A manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these “human hacking” scams tend to lure unsuspecting users into

exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions.

Software/App - Programs and applications that run on a computer or device, enabling users to perform specific tasks.

Software Update - A new version or patch released by software developers to fix bugs, add features, or improve security.

Spear phishing - deceptive and targeted form of cyberattack where the attacker pretends to be someone you know or trust, like a friend, colleague, or a company representative. They send you personalized and convincing messages, often through email, trying to trick you into revealing sensitive information, such as login credentials, passwords, or personal data.

URL (Uniform Resource Locator)- The web address used to locate and access specific websites or pages on the internet.

Username – A unique name used to identify a user's account on a computer or network. Your username is either your first initial last name OR first name.last name.

WiFi (Wireless Fidelity) - Technology that allows devices to connect to the internet and communicate wirelessly using radio signals.