

DePaul College Prep

2024-2025

Guidelines for Implementation of Acceptable Use Policy for Digital Information, Communication, and Technology Resources

ACCEPTABLE USE POLICY (AUP) and GUIDELINES

Scope:

DePaul College Prep provides employees and students access to technology devices, the Internet, and data systems for educational and business purposes. This Acceptable Use Policy (AUP) governs all electronic activity of students using and accessing the district's technology, Internet, and data systems regardless of the user's physical location.

Guiding Principles

- Online tools should be used in our classrooms, schools, and offices to increase community engagement, staff and student learning, and overall workplace efficiency.
- DePaul College Prep has a legal and moral obligation to protect the personal data of our students, families, and staff.
- DePaul College Prep should provide a baseline set of policies and structures to allow schools to implement technology in ways that meet the needs of their students.
- Nothing in this policy shall be read to limit an individual's constitutional rights to freedom of speech or expression or to restrict an employee's ability to engage in concerted, protected activity with fellow employees regarding the terms and conditions of their employment.

Student AUP & Contract

Copies of the AUP and the student contract for Internet use are included in the Student Handbook, which is given to all students at the beginning of the school year. By receiving this document, you agree to the Student Contract for Internet Use.

All use of DePaul College Prep's electronic network must be:

- in support of education and/or research, or
- for a legitimate school business purpose.

Use is a privilege, not a right. Students and staff members have no expectation of privacy in any material stored, transmitted, or received via DePaul College Prep's electronic network or devices. General rules for behavior and communications apply when using electronic networks. Appropriate and acceptable uses, ethics, and protocols are contained herein. School officials may monitor or read electronic communications and downloaded material, including files deleted from a user's account. DePaul College Prep employs network monitoring services known as Gaggle and Managed Methods. Any violations identified by Gaggle or Managed Methods of the AUP are emailed to the student's DePaul Prep email address, the Technology Department, the Counseling Department Chair, and the Deans of Students. The Deans of Students will determine the disciplinary consequences of violations, and the Counseling Department Chair will determine any additional actions, if necessary.

Access to Electronic Networks:

Electronic networks, including the Internet, are a part of DePaul College Prep's instructional program to promote educational excellence by facilitating resource sharing, innovation, and communication. **The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or legal action.**

DePaul College Prep is not responsible for any information that may be lost, damaged, or unavailable when using the network or for any information retrieved or transmitted via the Internet. Furthermore, DePaul College Prep will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Curriculum and Appropriate Online Behavior:

The use of DePaul College Prep's electronic networks shall (1) be consistent with the curriculum adopted by DePaul College Prep as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students and (2) comply with the selection criteria for instructional materials and library resource center materials.

As federal law requires, students will be educated about appropriate online behavior, including but not limited to (1) interacting with other individuals on social networking websites and (2) cyberbullying awareness and response.

DePaul College Prep's electronic network is part of the curriculum and is not a public forum for general use.

The use of iPads at DePaul College Prep should enhance students' learning experiences. Technology is integrated throughout all courses, and student devices are to be used first and foremost as learning tools.

Additionally, the following are guidelines for the expectation of using iPad responsibly:

- Bring a charged device to school every day.
- Store the device in the case at all times.
- Maintain the security of your iPad always. Never leave it unattended.
- Respect the property and privacy of others by not using another student's device or account.
- Use the device, app, and other information resources to support learning, complete school assignments, and understand how technology works.
- Use the Internet to gather information related to school and to communicate with other students, teachers, and experts about school work.
- Sound must be muted in class unless directed by the teacher.
- iPads may never be used in the bathroom or locker rooms.

CIPA

The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. Schools and libraries subject to CIPA may not receive discounts offered by the e-rate program unless they certify that they have an Internet safety policy that includes technology

protection measures. The protection measures must block or filter Internet access to pictures that are (a) obscene, (b) child pornography, and (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

DePaul College Prep fulfills these requirements in the following way:

1. Meraki Firewall Content Filter
2. Jamf Management System
3. iPad Digital Citizenship online class
4. Gaggle Software
5. Managed Methods Software

Guidelines for Technology Use

Privileges:

DePaul College Prep's electronic network is a privilege, not a right, and inappropriate use will cancel those privileges. The Administration will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. His or her decision is final. The Technology Director will work with all school administrators, and a school administrator will deal directly with the violator.

Unacceptable Use:

Staff and students are responsible for his or her actions and activities involving the use of computers and the network. Some examples of unacceptable uses include, but are not limited to:

- Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;
- Use personal or school-provided devices to airdrop files, photos, videos, etc, without the permission or approval of a faculty/staff member;
- Use of a Virtual Proxy Network (VPN) is strictly prohibited;
- Unauthorized downloading of software, regardless of whether or not it is copyrighted
- Using the network for private financial or commercial gain;
- Wastefully using resources, such as file space and bandwidth;
- Hacking or gaining unauthorized access to files, resources, or entities;
- Invading the privacy of individuals that includes the unauthorized disclosure, dissemination, and use of information about anyone that is personal, including images or video;
- Using another user's account or password;
- Posting material authored or created by another without his/her consent;
- Posting anonymous messages;

- Using the network for commercial or private advertising;
- Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
- Using the network while access privileges are suspended or revoked.

Network Etiquette:

Staff and students are expected to abide by the generally accepted rules of network etiquette when using electronic communication methods such as email, blogs, wikis, discussion boards, instant messaging, etc.

These include, but are not limited to, the following:

- Be polite. Do not become abusive in messages to others.
- Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
- Do not reveal students' or colleagues' personal information, including addresses or telephone numbers.
- Recognize that email is not private. The system's operators have access to all email. Messages relating to or supporting illegal activities may be reported to the authorities.
- Do not use the network in any way that would disrupt its use by other users.

No Warranties:

DePaul College Prep makes no warranties of any kind, whether expressed or implied, for its service. DePaul College Prep will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-delivery, missed deliveries, or service interruptions caused by negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. DePaul College Prep denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification:

The user agrees to indemnify DePaul College Prep for any losses, costs, or damages, including reasonable attorney fees, incurred by DePaul College Prep relating to, or arising out of, any violation of these procedures.

Security:

Network security is a high priority. If a user can identify a security problem on the network or Internet, the user must notify the Technology Department. The user should refrain from demonstrating the problem to other users. The user should also keep his/her account and password confidential. Attempts to log on to the network or Internet as a system administrator will cancel user privileges. Any user identified as a security risk may be denied access to the network.

Keep accounts and passwords confidential, and do not use another account.

Using VPNs while using DePaul College Prep's network is strictly prohibited as it jeopardizes the security protocols established by the school. Any attempt to knowingly or unknowingly use a VPN will result in disciplinary actions.

All teachers will be utilizing Jamf School, Schoology, and GSuite within their courses this year. Some teachers will use Office365, where Microsoft Office products are necessary for class. [Jamf School](#) is meant to focus on and enhance iPad use in class. It is a powerful teaching assistant that helps guide students through a lesson, allows teachers to provide educational and pertinent apps, and keeps them on track while in the classroom. Schoology is a learning management system (LMS) for K-12 schools, higher education institutions, and corporations that allows users to create, manage, and share content and resources. GSuite is the primary cloud-based creativity and communication tool.

Features Jamf School affords the teacher:

- Only functional during school days and hours.
- It allows a classroom teacher to quickly launch any app, website, or book on every student's device simultaneously while teaching.
- Allows teachers to group students by topic and launch a different app for each group.
- Using the app in the classroom, a teacher can lock devices to refocus students on the content being taught at that time.
- Allows teachers to lock devices into a single app, especially ensuring the integrity of online test-taking.
- The app's "End Class" feature disconnects student devices from the class while it is not in session.
- It does not collect or store student data, protecting student privacy.
- It does not require your child to download or install any spyware on his/her iPad.
- Does not grant faculty or staff access to any private files on the iPad.

Features of Schoology:

- **Flexible Instructional Tools** allow the teacher to easily differentiate instruction for students of different abilities. The material can be covered at a student's own pace or as a group, depending on the teacher and student's preference.
- **Calendar** - a way to manage personal and course events, ensuring communication for all.
- **Online Homework Submissions** - The in-line grading system allows the teacher to comment, annotate, and grade an assignment without downloading and then uploading the grade version.
- **Assignments and Events** - allows the teacher to create various assignments.
- **Tests and Quizzes** - allows instructors to create a variety of different types of questions for quizzes and tests.
- **Online Gradebook and Attendance** - allows the teacher to keep grades easily accessible and graded assignments and tests automatically input into the gradebook.

- **Customized Grading Options**—The teacher can grade using a numeric, alphabetic, or rubric system. The rubrics are completely customizable, including point value, descriptions, and naming.
- **Standards and Outcomes Alignments** - allows teachers to easily align content, assessments, and rubrics to Common Core, State Standards, or custom learning outcomes.

Features of GSuite

- **Collaborate Anywhere:** G Suite for Education integrates with Gmail and other Google apps, allowing users to collaborate in real-time.
- **Single Sign On:** Users can store their password and avoid having to sign in multiple times
- **Multimodal Communication:** Connect with email
- **Organize Tasks:** Schedule meetings create to-do lists and task reminders.
- **Work Offline:** Users can enable work offline and still work using G Suite apps without the internet. Once the user re-connects to the internet, all offline changes are updated.

Features of Office 365

- **Explore and Integrate:** Office 365 Integrates seamlessly with Microsoft Office and other Microsoft programs.
- **Stay Up and Running:** The cloud enables all apps to save virtually
- **Security:** Office 365 has built-in security and continuous compliance. You always know where your data is and who has access to it.
- **Organized:** When you use Office 365, the email, calendar, and contacts are all synchronized.
- **Real-time Collaboration:** Students and faculty can collaborate using Microsoft Word, Excel, and PowerPoint. Users can see real-time edits or additions other users make to a document.

Vandalism:

Vandalism will result in the cancellation of privileges and other disciplinary actions. Vandalism is defined as any malicious attempt to harm or destroy the data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

Telephone Charges

DePaul College Prep assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

Copyright Web Publishing Rules:

Copyright law and DePaul College Prep policy prohibit the re-publishing of text or graphics found on the web or School websites or file servers without explicit written permission.

- For each re-publication (on a website or file server) of a graphic or text file produced externally, a notice at the bottom of the page must credit the original producer and note how and when permission was granted. The notice should also include the source's web address.
- Students and staff producing web content must have written permission from the original producer before adding the material to their web page.
- The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the consent. The website manager displaying the material may not be considered a source of permission.
- The fair use rules governing classroom student reports are less stringent and permit limited use of graphics and text.
- Student work may only be published if there is written permission from both the parent/guardian and the student.

Use of Email:

DePaul College Prep owns and controls its email system and its constituent software, hardware, and data files. DePaul College Prep provides email to aid students and staff members in fulfilling their duties and responsibilities and as an education tool.

- DePaul College Prep reserves the right to access and disclose the contents of any account on its system without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an email account is strictly prohibited.
- Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.
- Electronic messages transmitted via DePaul College Prep's Internet gateway carry with them identification of the user's Internet "domain." This domain is registered and identifies the author as being with DePaul College Prep. Therefore, great care should be taken in the composition of such messages and how such messages might reflect on the name and reputation of DePaul College Prep. Users will be held personally responsible for the content of any email messages transmitted to external recipients.
- Any message received from an unknown sender via the Internet should either be immediately deleted or sent to spam. Downloading any file attached to any Internet-based message is prohibited unless the user is sure of that message's authenticity and the nature of the file so transmitted.
- Use of DePaul College Prep's email system constitutes consent to these regulations.

Internet Safety:

- Internet access is limited to only those acceptable uses, as detailed in these procedures.

- Staff members shall supervise students using DePaul College Prep Internet access to ensure that they abide by the Terms and Conditions for Internet access contained in these procedures.
- Each DePaul College Prep device with Internet access has a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children’s Internet Protection Act and as determined by the President or designee.
- The technology network administrator shall monitor the Internet for students and staff.

Apps for School Use (others may be added during the year)

<i>Name</i>	<i>Function</i>	<i>Requested Permissions</i>
Chrome/Safari	Internet browser	Camera, microphone, Siri
Schoology	Learning management system	Siri
Zoom	Virtual meeting app	Camera, microphone, Siri
Gmail	Email	Siri
Google Drive	Cloud-based storage	Siri
Google Docs	Create/open text documents	Siri
Google Sheets	Create/open spreadsheets	Siri
Savvas	App to download textbooks	Siri
Google Keep	Create/open notes and lists	Siri
Google Calendar	Calendar	Siri
Google Slides	Create/open slides	Siri
Flipgrid	Video discussion app	Camera, microphone, Siri
Notability	Note-taking app (paid)	Siri
TurnItIn	Anti-plagiarism app	Siri
Socrative	Cloud-based student response app	Siri
Adobe Photoshop	Image editing app	Siri
Adobe Illustrator	Design app	Siri

Jamf School	Mobile device management solution	Hardware Specifications Installed Applications Total Disk Space Usage Services Running Available Software Updates Local User Accounts and Login/Logout Timestamps Security Status (Firewall, SSH, etc) Primary User Information Campus Building Location No personal information is collected, such as contents or names of personal files (documents, photos, music, email, etc.) or any browsing history.
-------------	-----------------------------------	--

Authorization for Electronic Network Access:

Each student and his or her parent(s)/guardian(s) agree to these provisions while enrolled or visiting DePaul College Prep

All users of DePaul College Prep’s computers and means of Internet access shall maintain the confidentiality of student records. Before confidential student information is loaded onto the network, reasonable measures to protect against unreasonable access shall be taken.

If any student or staff member fails to follow the terms of the *Authorization for Electronic Network Access* or this policy, they will lose their privileges, face disciplinary action, and/or appropriate legal action.

LEGAL REF.: No Child Left Behind Act, 20 U.S.C. §6777. Children’s Internet Protection Act, 47 U.S.C. §254(h) and (1). Enhancing Education Through Technology Act, 20 U.S.C §6801 6751 et seq. 47 C.F.R. Part 54, Subpart F, Universal Service Support for Schools and Libraries. 720 ILCS 135/0.01.