Princeton Day School
Acceptable Use Policy
for US, MS and LS

As stated in each 2019-2020 PDS division handbook

Upper School Acceptable Use Policy

PDS Upper School Technology Acceptable Use Policy (AUP)

The following Acceptable Use Policy (AUP) applies to all technology resources owned or managed by Princeton Day School, including but not limited to the network, email and learning management systems, and all PDS hardware. These rules apply to any devices used on PDS premises or at School functions, any devices on the School's network, and all School-owned devices. Any activity, regardless of the device or location, that involves other members of the PDS community is subject to this policy. Technology resources are provided by Princeton Day School for the primary purpose of conducting academic work and facilitating communication among PDS faculty and students. The School expects that students will treat these resources and others who use them with respect and for what they were intended. Access to PDS campus technology, including the network, is a privilege rather than a right, and appropriate usage is governed by the behavioral standards outlined in the PDS Honor Code, Upper School Handbook, and this AUP.

Academic and personal integrity are essential to the PDS learning community, and thus these values should also extend to behavior involving PDS technology. The same ethical standards apply to digital situations that apply to all other spheres of life at PDS.

For example:
Just as you may not steal another student's belongings, you may not steal their password or their online identity. Both are violations of the PDS Honor Code. Just as we expect you to treat others with respect and civility when speaking to them in person, we expect the same standards of respect and civility when interacting with others online.

Just as you represent PDS when you are off campus, you represent PDS whenever and wherever you engage online, even when you are not using the PDS network.

PDS has the responsibility to monitor its network, and thus all activity is logged. It also has the right, when requested by a faculty member, dean, or administrator, to review student activity on the network, including email, if there is concern about possible

impropriety or violation of school rules. As a matter of course, PDS does not read the content of student emails without cause, however there is no guarantee of privacy with use of the network. The network is the property of PDS, and the School reserves the right to monitor a student's network use at any time and for any reason. In order to protect the network from malicious parties and shield students from inappropriate content, student access to the internet is also regulated by a web filter. Downloads for academic purposes are allowed and logged.

The PDS network is monitored by members of the School's Technology Department, who serve along with the Class Deans, Dean of Students, and Head of Upper School to uphold the AUP as defined below.

- **Acceptable Use Guidelines:** Those who employ PDS technology resources, including the network, are responsible for upholding the following standards of behavior. Please refer to Section VII of the US Student Handbook for an explanation of violations of "Student Behavioral Expectations" and the role of the Judiciary Committee in addressing violations.
    - Students must abide by appropriate standards of etiquette and respect when interacting with others online. Threatening or abusive behavior and harassment are classified as primary offenses and will not be tolerated at PDS or on the PDS network (see PDS US Handbook). Posting messages to Schoology groups, public or private email lists, or other digital forums using offensive, threatening, abusive, bullying or harassing language and/or obscenities (even with alterations or missing letters) are considered inappropriate. *Students who witness or receive words or media considered offensive or harassing should notify their advisor, class dean, the Dean of Students, or the Head of Upper School.*
    - Engaging in any activity online or using PDS resources that is potentially damaging to oneself, to others or to the School is considered unacceptable.
    - Vandalism of PDS technology resources, whether petty or significant, is always unacceptable. Damage, abuse, dismantling or unauthorized modification of hardware or software (including the network) is considered vandalism.
    - Students must not use the PDS name or logo on communications or media that are not officially controlled, operated or sanctioned by the School.

- Students must not be involved in any activities that promote violence or that are prohibited by law, including the transmission of sexually explicit material.
- Students must respect and abide by the copyright and licensing agreements of published software. These agreements usually state that copying, altering, or distributing licensed software is illegal.
- Students must not copy or download any unauthorized applications through the PDS network, including but not limited to games and unlicensed software.
- Attempting to access or “hack” someone else’s email account or personal computing device is considered a form of theft, which is a primary offense.
- Regardless of whether or not permission is granted, students must never log into the accounts of others. PDS network accounts are for individual use only, and account credentials must always be kept secret. Similarly, masquerading as someone else or otherwise attempting to hide one’s own identity is considered lying (pretending to be someone else online) and/or theft (falsely assuming or stealing another person’s online identity), which are primary offenses.
- Students must not make any attempt to break, alter or infiltrate the School's computer or network security systems. This is a form of vandalism treated as a primary offense.
- Students must abide by -- and not attempt to circumvent -- any other rules that the School deems necessary to enforce the AUP such as private chat and email restrictions, network access protocols, and account access limitations.

Middle School Acceptable Use Policy

School-Owned iPad Use

Technology is an important part of the learning process that, when managed well, contributes greatly to student success. Your online work, activities, interactions and posts over time become an important profile or "digital footprint" for you. By using technology resources in appropriate ways, you are developing a positive digital footprint that will follow you throughout your PDS career and beyond. We strongly encourage students to utilize their iPads when taking notes, preparing homework, writing papers and assignments, working on research projects, presentations, and other aspects of their academic life at PDS. Computer use in the middle school is a privilege and should be treated as such. The following guidelines are designed to help students make safe and effective use of technology in the middle school.

Acceptable Use Guidelines

- PDS email accounts are provided to all middle school students for academic purposes and for communicating with teachers. No middle school email accounts can receive email from a non-PDS account.
- During class time, resource periods, iPads, computers and email accounts should only be used for academic work. Checking email, playing computer games, or browsing the internet during these times is not an appropriate use of a student's academic time or the school's technology resources.
- iPads may not be used during lunch or recess.
- Using a school iPad to send instant messages, texts, or email through a non-PDS email account or service is not permitted at any time.
- PDS manages its iPads and computers. Any attempt to interfere with the management of school-owned devices and computers is unacceptable.
- Students are not permitted to download apps that have not been purchased by the School, such as games or social media apps.
- Any action intended to gain unauthorized access to online resources or accounts, to obtain login information of other users, or to in any way disrupt performance of technology systems, is prohibited.
- Using any computing device for academic dishonesty, vandalism, theft, harassment, or abusive behavior is a serious breach of our community code of conduct.

- Material that is sexually explicit, promotes hate speech, or panders to bigotry tends to degrade other people and is prohibited. Images visible from any device must be free of all messages that promote tobacco, alcohol or drug use, or messages that are demeaning to any group of people. Any action that is potentially harmful to oneself, the School or others is unacceptable.
- Failure to follow the guidelines for use may result in a loss of computer or iPad privileges or more serious disciplinary action. When using PDS computers or the PDS Network you are, by extension, representing your school and a high standard of personal responsibility is required.
- Treat all school property, including computers, iPads, and other electronic devices with respect. If any computing device, including a school-issued iPad, is damaged, it must be reported to a teacher immediately and the IT office alerted at the first opportunity.
- All information created, used, or stored on school resources is subject to review by school administration. This includes school-owned hardware and PDS accounts, or personally owned hardware on the school's network or school property.

Safety Guidelines

- Be kind. Be as polite as you would be in person, and never use inappropriate or offensive language.
- Don't give out your or anyone else's personal information such as a picture, full name, address, telephone number, or school name without your parent's or guardian's permission.
- Don't meet in person with anyone you have first met online.
- All content produced on an electronic device should show respect for others and be used for academic purposes only. Use of technology to capture images, audio, or video without the permission of a teacher is not allowed.
- Don't share your email or Internet accounts or passwords with others, even close friends, and never use someone else's account, username, or password to go on-line.
- Don't respond to any messages or posts that are mean or in any way make you feel uncomfortable. Tell your teacher or parent immediately if you receive such a message or come across any information that makes you feel uncomfortable.
- Don't download unknown attachments or click on or accept popup offers as they may contain destructive viruses, and don't send or forward junk mail, spam or chain letters.

- Never open an email attachment that you are not expecting or that seems suspicious. If you are uncertain, ask an adult first. Do not click on links or advertisements that promise products or services, and never type a username, password or other information about yourself in response to an email. All of these can be used by people who would like to steal your information or damage your device or the school. If you suspect you may have mistakenly opened a problematic attachment, clicked a link, or entered information, be sure to tell a teacher immediately.
- Understand that you continuously represent Princeton Day School whenever and wherever you use email and Internet resources, even if you are using these resources away from or outside of the School's network.

Personal Electronics

Personal electronics can be a distraction for our students. While we wish students would simply leave their phones and devices at home, we understand this to be an unrealistic expectation. To help maintain a conducive atmosphere for learning, we are asking everyone to adhere to the following protocols.

1. Non-school owned iPads must be left at home.

2. Laptops must be left at home.

3. Cell phones and Wi-Fi Enabled Devices

- Must be powered off and left in lockers or backpacks upon arrival to school.
- Students may not send or receive text messages or phone calls during the school day (upon morning arrival to 3:20 p.m.).
- During school hours, parents are to call the Middle School office if they need to get in touch with their child.
- Students may not use the camera to take photos or videos while at school without teacher permission.
- Wi-Fi enabled devices being used during school hours will be turned over to the dean.

4. eReaders can be used with teacher permission.

5. Personal gaming devices must be left at home. Gaming should not take place at school on any device.

Lower School Acceptable Use Policy

As a part of my schoolwork, my school gives me computers and iPads for my work. I will follow my class and school rules when using a computer or ipad. To help myself and others, I agree to the following promises:

1. I will use the Internet only with my teacher's permission. When I am looking for something on the internet, I will only search for what my teacher has asked me to find.
2. I will not give my password to anyone else, and I will not ask for or use anyone else's password.
3. I will not put my name, address, telephone number, or any other personal information about myself or anyone else on a website.
4. I will not take or upload an image or video of myself or others without my teacher's permission.
5. I will be polite and considerate when I use the computer; I will not use it to annoy, be mean to, or bully anyone.
6. I understand it is a privilege to use a computer and iPad. I will do my very best to take care of them. I will respect others' work on computers and iPads.

The PDS Lower School has initiated a 1:1 iPad program with our first, second, third and fourth graders. Students share iPads in Pre-Kindergarten and Kindergarten. Students have access to iPads during the school day. By integrating the iPad into the curriculum, our students are empowered to take ownership over their learning, which leads to greater engagement. The following guidelines have been designed to help the students understand how to use the technology safely and effectively.

iPads are to be used for educational purposes only and as directed by the teachers:

- Online games or websites that are not related to education are not to be used.
- Students may not record sound or take photos or videos unless it is for educational purposes. Students must get permission from their teacher beforehand.
- Students will be given a Princeton Day School email account to be used for educational purposes only. Any other email accounts must not be accessed at school unless permitted by a teacher.

iPad Home Use Guidelines
(distributed with School-issued iPads March 2020)

Only a basic internet filter is applied at home on the iPads. You do not need to do anything with the iPad to have the filter work. Filters are never perfect, and children should be monitored when they are online.

1. The primary use of the iPad is to complete work assigned by PDS teachers.
2. Wash hands before using the iPad. Keep food and drink away from the iPad at all times.
3. Be sure to store the iPad on a clean, flat surface. Do not store it on the floor, on a pile of books or on the edge of a table.
4. Always keep the case on the iPad.
5. Keep the iPad and the case clean. Do not permanently alter it in any way. This includes putting on stickers or drawings on the case or iPad.
6. Report any problems, damage or theft immediately to Carol Olson (colson@pds.org).
7. Do not remove any serial numbers or identification placed on the iPad or case.
8. If you need to clean the iPad screen, only do so with a soft, dry, anti-static cloth or with a screen cleaner designed specifically for LCD-type screens only.
9. When campus schooling begins again, it is expected that the iPad and its charger will be returned to PDS.
10. Families will be charged a fee if iPads are lost or damaged.
11. During these uncertain times, there are always possibilities of internet outages or interruptions with our filtering service.
12. Please monitor your child's use of any devices in your home, including their PDS iPad.