



USP INFORMATION TECHNOLOGY POLICY 2021

Acceptable use

Through technology we equip children to participate in a rapidly-changing world where work and leisure activities are increasingly transformed by technology. We enable them to find, explore, analyze, exchange and present information. We also focus on developing the skills necessary for children to be able to use information in a discriminating and effective way. Technology skills are a major factor in enabling children to be confident, creative and independent learners.

The aim of this policy is to foster appropriate use of digital technologies and to establish attitudes and behavior that will protect the students, the United School of Panama community and the school's IT resources.

In PK and Kinder, shared iPads are provided for student use under the guidance of the classroom teachers. In grade 1, this is expanded to a 1:1 iPad program.

Parents: please discuss the policy rules with your child to ensure he or she understands them thoroughly. Feel free to simplify the rules for your child or to contact the school for advice in this area.

Technologies and Resources Covered

The policy is in two parts:

- Specific rules relating to direct use of the school's IT resources
- Guidelines for the use of digital technologies both within and outside the school environment

Information Technology Resources at United School of Panama (USP)

USP's information technology resources, including Internet access, are provided for educational purposes. Students are responsible for good behavior in this virtual environment just as they are in the physical school environment.

- All students have access to i-Pads, laptops and other digital technologies provided by the school.
- All students have access to shared local network resources and the Internet.



- Students in PK and K use generic accounts managed by the class teacher.
- Students in Grade 1 and above have individual network accounts which are password protected.
- From Grade 1 to Grade 5, these passwords are controlled by IT initially. Students may be able to change them as they access the system for the first time.
- Students in Grade 1 and above have **USP** email accounts on the domain usp.edu.pa.

Whenever a student accesses the **USP** network they implicitly accept the following terms:

USP network and Internet access

Please remember that when you log on to the school's computers you are bound by the 'Acceptable Use of IT' Policy. This Policy is in place to protect our students and our network. Any attempt to bypass the access permissions set by the school to Internet sites or network locations will be considered a serious breach of this Policy. The school can monitor user accounts and Internet access and keep logs of inappropriate activities. Please use our IT resources thoughtfully and responsibly.

Supervision and Monitoring of IT Resources

School and network administrators monitor the use of IT resources to help ensure that uses are secure and conform to the school's mission. The school reserves the right to examine, use and disclose any data found on the school's networks or information systems in order to further the health, safety, discipline or security of any student or other person, or to protect property.

They may also use this information in disciplinary actions.

Policy Regarding Use of IT Resources

Please remember that access to **USP** IT resources is a privilege, not a right, and that access requires responsibility. Individual users of the school's resources are responsible for their behavior, actions and communications. The following rules have been established and access to the school's systems implies acceptance of these rules.



Students are expected to:

Respect the privacy of others and the security of USP Schools System.

Only use your user ID and password – do not use another person’s user ID and password.

- Do not share your password with others.
- Do not try to learn other people’s passwords.
- Do not try to disrupt, interfere with, or destroy computers, networks, equipment, or information.
- Do not access, store, or transmit information that is hateful, harassing, insulting, offensive, false or defamatory, sexually explicit, obscene, or otherwise inappropriate.
- Do not interfere with the academic or work activities of others.

Respect the copyrights and licenses of software and information.

Do not copy, download, install, or distribute software in violation of copyright laws or licensing agreements.

Do not copy, share, or transmit information in violation of copyright laws.

Respect the integrity of our computers, networks, and equipment.

Do not try to access computers or networks for which you do not have permission.

Do not install software on an USP equipment. Do not connect an equipment, network, or device to a USP network.

Do not bypass any security system or feature put in place to protect, monitor, or restrict access to information (for example, do not use an Internet proxy server to avoid USP web content filters). Do not create, download, install, or use software or equipment that can be used to “hack into” or damage a computer or network.

Do not change, remove, or damage computers, networks, or equipment. Do not use software or hardware to keep USP staff from accessing information.

Use information systems for authorized purposes only.

Only use i-Pads, computers and networks for academic activities – not to play non-academic games or for prohibited activities. Do not access the Internet from USP facilities using any network or computer not provided by USP.



Protect information from loss, theft, disclosure, or unauthorized use.

Do not access or share information for which you do not have permission, or help others to do so.

Do not give information to others that could help them gain access to the computers or networks of the **USP** systems.

Take care of the computers and equipment assigned to you to prevent loss, theft, damage, or unauthorized use.

Report any loss, theft, unauthorized disclosure, or unauthorized access to a teacher or administrator.

Consequences for Violation

Violations of these rules may result in disciplinary action, including the loss of a student's privileges to use the school's IT resources.

Guidelines for Use of Digital Technologies

New digital technologies mean that access to **USP** IT resources extends beyond the physical boundaries of the school and that the distinctions between school and home are not so clear cut as they once were. Please read carefully the following guidelines and notes on the use of digital technologies as they apply to staff, students and the wider **USP** community.

Classroom use of Social Media

Students are expected to refrain from accessing social network sites during school hours unless expressly asked to do so as part of a class activity. Teachers are required to limit class activities to approved online tools.

Classroom use of other public online applications

Where online tools are used to share information with students or about the class or school, appropriate care must be taken regarding content and security. Specifically, no photos should include names of the children in the photos and no student/parent names or contact details should be displayed.

Social media relationships with students, alumni and parents



Staff are instructed not to initiate or accept social media “friend” requests from current students (of any age) or former students under the age of 18. Staff are discouraged from “friending” parents of current or prospective students due to the inherent conflicts of interest that may arise.

Social networking sites

Social networking sites usually have a minimum age for membership. Staff who see children under this age using these sites are asked to report the incident to the School Academic Director.

Privacy settings

On most sites, privacy settings can be changed at any time to limit search ability and access to profiles. Students should be prudent in allowing access to their online content, consistent with other requirements of this policy.

Use of USP email accounts

Messages sent from usp.edu.pa email addresses should not include content that would reflect poorly on the sender or the school.

Data protection

Make sure that your network account is protected with a strong password. Do not share this password with anyone. Change your password immediately if you have any reasons to believe your account has been or may be compromised (or shared).

E-safety and Digital Citizenship

All students (and parents) should be sure that they understand all the risks that digital technologies create and have clear strategies in place to minimize the impact of these risks. E-safety is taken very seriously at **USP**. It is incorporated into the computer science curriculum.

Emerging technologies

As new technologies and technology initiatives emerge, it may be necessary to make changes to this policy. Where such changes are significant these will be communicated directly to students and their parents.