European School Acceptable Use of ICT Policy

Review Frequency: Annual
Prepared by: Digital Transformation Permanent Committee
Policy written in: September 2018
Last reviewed by: Digital Transformation Permanent Committee
Last review date: November 2024

Sophio Bazadze
Director

GEORGIA "EUROPEAN SCHOOL" Ltd 205172917

2 I. Skhirtladze Str. Tbilisi, 0177, Georgia
Tel: (032) 239 59 64,
info@europeanschool.ge
www.europeanschool.ge
ს/კ : 205172917

Table of Contents

European School Acceptable Use of ICT Policy

All students of "European School" Ltd. (hereinafter - "European School" or "School") must comply with the terms and conditions expressed in this document when using computers, IT services and IT equipment in the European School.

This document, which is available through the school's official website and emailed by the school to each student's parent /guardians, specifically states the rights and responsibilities of all for appropriate communication, education and research and collaborative work.

The use of electronic devices and IT services is a privilege, not a right, and inappropriate use may result in the cancellation of your privilege and other appropriate disciplinary consequences.

Students must

- use school computers and IT equipment respectfully and carefully.
- keep personal data and login data in secret.
- not use school computers to download, duplicate, modify and/or distribute copyrighted materials (in accordance with Law of Georgia on Copyrights and Related Rights).
- not use computers to share illegal content over the local area network or through the internet.
- not use computers to share personal data (name, birth date, personal photos) of themselves, classmates or teachers to the public (for example, via the internet).

Authorized Use

Students are authorized to use school available computers and laptops as designated by their teachers or school staff in accordance with the rules outlined in this policy document.

Students are permitted to use AI-based tools only for educational purposes and under teacher supervision. The use of such tools must align with ethical guidelines, including proper attribution and avoiding plagiarism.

Students will be educated on the ethical implications of using AI tools, including understanding biases, avoiding misuse, and maintaining transparency in their work.

Login Information

All students have logins and passwords for access to the school’s emails and e-portals. When a student is finished using an email or e-portal, the student must log out.

Password Secrecy

Students have the responsibility to protect their passwords. This means that a student must not give his/her login information to other people and must not log in to the computer system for other people. Students are expected to report when they notice other people using another person’s login and password for access to the school’s computer systems. The school administration has the right to deactivate any login that is suspected to be compromised.

A student is not allowed to use someone else's username and password to access the school's emails or e-portals. Students are not allowed to obtain passwords of other users by any means.

Computer Use for School Purposes Only

The school computer systems and network (computers, internet access, software, external devices, cameras, video cameras, printers, scanners, etc.) may only be used for school-related purposes. This rule applies during class, during break and lunch times, before school and after school.

Copyrighted Materials

Students must not use the school computer systems and/or network to duplicate, share or modify copyrighted digital media without express written permission of the copyright holder or copyright administrative organization and permission of a teacher or school staff.

Network Etiquette and Privacy

Students are expected to adhere to the generally accepted rules of network etiquette. These rules include, but are not limited to the following:

- Be polite: Never send or encourage others to send abusive messages.
- Use appropriate language: Remember that you represent the school on a global public system. You may be alone with your device, but what you say and do can be viewed by others. Never swear or use vulgarities or other inappropriate language. Illegal activities of any kind are strictly forbidden.
- Privacy: Do not reveal personal data to anyone, especially your home address or personal telephone number, or those of other students.
- Password safety: Do not reveal your password to anyone. If you think someone has obtained your password, change it and contact a member of the ICT support team.
- Network use: Email, internet and network use may be monitored at any time by designated staff. Regular audits are conducted to detect inappropriate and illegal use.
- Disruptions: Do not use the network in any way that would disrupt use of services by others.
- Students and parents must provide written consent before using school-provided tools that collect personal data. This ensures compliance with data protection laws and informs users about how their data will be processed.
- Any suspected breaches of data privacy, unauthorized access, or inappropriate behavior online must be reported to the ICT support team immediately. A designated team will investigate incidents and apply appropriate corrective measures.
- Students will participate in digital citizenship workshops to learn about respectful online behavior, the importance of maintaining privacy, and the ethical use of technology.
- The school will run annual digital citizenship programs to educate students on the ethical use of technology, privacy protection, and respectful online communication.
- The school will establish a clear, anonymous reporting mechanism for students and staff to report cyberbullying, inappropriate online behavior, or other ICT-related concerns.

System Configurations

- Students must not change the installation and configuration of the school computer systems (both hardware and software) and network.
- Students may only restart computers with the permission of teachers or school staff.
- Students must not access, modify, delete, or destroy another user's files.
- Students must not install software on any school computing device.
- Students must not introduce viruses, Trojans, worms, rootkits, key loggers, etc. to the school's computer systems and network.
- The school reserves the right to conduct regular audits of network activity and device configurations to ensure compliance with the policy and maintain a secure digital environment.

Chat Services and Social Networking

Students are not permitted to use social networking websites or chat services through the school network except when the teacher gives permission.

Bring Your Own Device

General Usage

European School provides the opportunity for students throughout Secondary and High School (From grade VI to Grade XII) to bring a personal laptop/tablet to school to use as an educational tool. The use of this laptop/tablet will be at the teacher's discretion.

1. Students must obtain teacher permission before using a personal laptop/tablet during classroom instruction or from the librarian when studying in the library.
2. Student use of a personal laptop/tablet must support the instructional activities currently occurring in each classroom and lab.
3. Students must turn off and put away a personal laptop/tablet when requested by a teacher.
4. Students should be aware that their use of the laptop/tablet could cause distraction for others in the classroom, especially in regard to audio. Therefore, audio should be muted, since headphones should not be used during instructional time.
5. The laptop/tablet should be used for educational activities only.
6. In the case that students and parents/guardian do not agree with this policy, student is not allowed to bring her/his own laptop/tablet or to use others.
7. Heads of program reserve the right to suspend the use of laptop/tablet in the classrooms.
8. Students must complete an annual cybersecurity awareness training to understand the importance of safeguarding their devices, data, and login credentials against potential threats such as phishing or malware.
9. Students are encouraged to adopt sustainable practices, such as reducing unnecessary printing, limiting device usage during non-instructional time, and turning off devices when not in use.
10. The school provides alternative access to ICT resources for students who may not have personal devices. This ensures equitable opportunities for all students to participate in digital learning.
11. Students are encouraged to practice digital wellbeing by balancing screen time with physical

activities, engaging in mindful technology use, and taking regular breaks from digital devices.

12. In situations requiring remote or hybrid learning, students must adhere to online classroom etiquette, including muting microphones when not speaking, using appropriate backgrounds, and refraining from unauthorized recording of sessions.

Consequences of General Usage

If students refuse to comply with the above guidelines, the following consequence will apply. Student infractions will be documented as a referral for each offense.

1. First offense – laptop/tablet will be confiscated and given to the program coordinator or homeroom teacher. Parents/Guardian and student will be called for a meeting with program coordinator and/or home room teacher. The meeting may not happen the very same day of the offense but within a week. After the "educational" meeting laptop/tablet will be returned to the student.
2. Second offense – laptop/tablet will be confiscated and given to the program coordinator or homeroom teacher. Parents/Guardian and student will be called for a meeting with program coordinator and/or home room teacher. The meeting may not happen the very same day of the offense but within a week. After the "educational" meeting laptop/tablet will be returned to the student but student will not be allowed to bring her or his laptop/tablet to school or to use others.
3. In cases where students cause a data breach due to negligence or intentional misuse of devices, additional consequences, such as loss of access privileges or involvement of legal authorities, may apply depending on the severity of the incident.
4. In cases of repeated violations, the school may impose extended restrictions on ICT use, and students may be required to participate in remedial workshops focused on responsible technology use.
5. The school will ensure ICT resources are accessible to students with disabilities by providing assistive technologies and tailored support as needed.

Student Responsibility

1. Laptop/tablet must be charged at home. Students may not charge their laptop/tablet batteries in the school.

2. Students should take all reasonable steps to protect against theft or damage of their personal laptop.

3. Parents/Guardians are encouraged to insure their child's personal laptop/tablet against loss, theft, or damage, as the school will not be liable for any such incidents.

4. Parents/Guardians are encouraged to actively participate in discussions about technology use at home and school to reinforce safe and responsible online behavior.

Regular Policy Updates

This policy will be reviewed annually to ensure it reflects emerging technological trends and aligns with the latest legal and educational standards.

Bibliography

Children's Internet Protection Act (CIPA). (2000). *Federal Communications Commission Guidelines for Internet Safety in Schools*. Washington, D.C.: U.S. Federal Government. Available at https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

Department for Education (DfE). (2020). *Keeping Children Safe in Education: Statutory Guidance for Schools and Colleges*. London: Department for Education. Available at https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

International Society for Technology in Education (ISTE). (2019). *ISTE Standards for Students: Empowering Learners in a Connected World*. Eugene, OR: ISTE. Retrieved from https://www.iste.org/standards/iste-standards-for-students

UNESCO. (2021). *ICT in Education Policies and Practices: A Global Perspective*. Paris: UNESCO Publishing. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000377076

Common Sense Media. (2018). *Digital Citizenship Curriculum: Tools and Resources for Schools*. San Francisco: Common Sense Media. Available at https://www.commonsense.org/education/digital-citizenship

European Commission. (2018). *Digital Education Action Plan: Promoting Technology Use in Schools Across Europe*. Brussels: European Union Publications. Retrieved from https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en

Parkstone Grammar School. (2021). *ICT and Internet Acceptable Use Policy*. Bournemouth: Parkstone Grammar School. Retrieved from https://www.parkstone.poole.sch.uk

Thorndown Primary School. (2018). *ICT Acceptable Use Policy for Staff and Pupils*. Cambridge: Thorndown Primary School. Retrieved from https://www.thorndownprimaryschool.co.uk