School e-Safety 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

School e-Safety Policy

Why is Internet Use Important?

The purpose of using the Internet in "European School" Ltd. (hereinafter "European School" or "School") is to raise educational standards, to promote students' achievements, to support the professional work of staff and to enhance the school's managementinformation and administration systems.

Internet use is an integral part of the school curriculum and is very important tool for learning process.It is an essential element in 21st century school education. Therefore, access to the Internet is an essential for students to get High quality education.

Our school has a responsibility to provide students with high-speed Internet connection. Students willuse the Internet in the school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use in education goes beyond access to resources; it also fosters digital citizenship by teaching students ethical online behavior, critical thinking about online content, and respect for others in digital spaces. The school is committed to ensuring all students, including those with disabilities, have equitable access to internet-based learning opportunities.

To ensure equitable access, the school will support students who lack access to digital devices or the internet. Programs will also be available to educate parents or guardians on how to effectively use technology to assist their children in learning.

Benefits of using the Internet in education process include:

- Access to world-wide educational resources including scientific articles, museums, art galleries, libraries etc.
- Tools like websites, apps, learning games, e-books, and virtual tutoring help the student learnat their own pace.
- Educational and cultural exchanges between students world-wide.
- Access to experts in many fields for students and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Online courses from leading institutions
- Collaboration across support services and professional associations; improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administration data with the school community.
- Communicate with parents.
- Valuable networking and learning opportunities from peers from other schools, business leaders, industry experts, and others.
- Use e-learning platforms, tools, websites to communicate with teachers, students.
- Etc.

Scope of the policy

This policy applies to all members of the school community, including staff, students, parents and visitors, who have access to and are users of the school IT systems.

In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. ‘Parents’ includes students' careers and guardians. 'Visitors' includes anyone else who comes to the school. Both this policy and the ES Acceptable Use of ICT Policy cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, whiteboards and digital video equipment); as well as all devices owned by students, staff, or visitors and brought onto school premises including personal laptops, tablets, and smartphones.

The policy outlines clear expectations for all groups: students, staff, parents, and visitors. Non-compliance with the policy will lead to specific consequences, such as restricted access to school IT systems or further disciplinary action. Visitors accessing school IT systems must receive prior authorization and adhere to the Acceptable Use Policy.

Authorized Internet Access

- The school maintains a current record of all staff and students who are granted Internetaccess.
- The school provides all staff and students with emails.
- All students and parents must read the “European School Acceptable Use of ICTPolicy” sent to them on email by the school before using any school ICT resource.

World Wide Web

If staff or students discover unsuitable sites, the URL (address), time, content must be reported to the IT manager, who is responsible for school e-safety.

Students should be taught how to research information in the internet and how to validate it before accepting its accuracy.

Email

Students and staff may only use approved e-mail accounts on the school system.

Students must immediately tell a teacher if they receive offensive e-mail. Students must not disclose personal information or others in e-mail communication or arrange to meet anyone without specific permission.

E-mail sent to external organizations should be written carefully before sending.

Social Networking

Students at the school will be advised to never give their personal data of any unknown person. Students should be advised not to place personal photos on any social network space.

Students at the school should be taught and encouraged to set strong passwords, deny access to unknown individuals and block unwanted communications.

Students and staff are encouraged to report any incidents of cyberbullying or harassment encountered on social networks. The school will provide clear instructions on how to report suspicious or harmful content. Social media education will include privacy settings, recognizing fake profiles, and responsible sharing practices.

Management of emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carriedout before use in school is allowed.

Students must be informed that:

- Mobile phones are not allowed for personal use during the lessons or formal school time.
- The sending of abusive or inappropriate text messages is forbidden.

Emerging technologies will be evaluated not only for educational benefit but also for privacy and security implications. A consultation process with teachers, students, and parents will guide the adoption of new tools. AI-based platforms will be assessed for ethical use, data privacy compliance, and transparency.

The school will ensure that the integration of AI and other emerging technologies is done ethically, prioritizing transparency, privacy, and educational value. Students and staff will receive training to understand the benefits and limitations of these tools.

Publishing Students' Images and Work

Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.

Students' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.

Written permission from parents or careers will be obtained before photographs of students are publishedon the school Web site.

Student work can only be published with the permission of the student and parents.

In addition to photographs, videos taken during virtual classes or other events must adhere to the same privacy standards. All multimedia content will be securely stored and deleted when no longer needed, as per the Data Protection Policy.

Information System Security

School ICT systems capacity and security will be reviewed regularly. Virus protection will be installedand updated regularly.

There is strong firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for schoolwork or research purposes, students should contact the e-Safety Officer for assistance.

Security strategies will be discussed with the School Governance.

All users of the school IT systems will undergo periodic cybersecurity training, focusing on phishing, password management, and identifying malware. Multi-factor authentication (MFA) will be implemented for accessing sensitive data or systems, adding an extra layer of security.

In the event of a major cybersecurity incident, the school will implement a structured response plan, including:

- Immediate containment and mitigation measures.
- Notifications to relevant stakeholders.

- Reporting to authorities as required.
- A thorough review to prevent future incidents.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the school Data Protection Policy.

The school will actively educate staff and students about their data protection rights under applicable laws. The policy will ensure clear guidelines for rectifying, deleting, or transferring personal data, as well as for data breach notifications.

Data storage and processing

The school takes compliance with Data Protection legislation very seriously. Please refer to the Data Protection Policy for further details.

Staff and students are expected to save all data

relating to their work to their school Google Drive account or to the school's central server.

The school expects all removable media (USB memory sticks, CDs, portable drives) to be encrypted before being used or at least protected with password.

Staff may only take information off-site when authorized to do so, and only when it is necessary and required in order to fulfil their role.

No personal data of staff or students should be stored on personal memory sticks or personal onlinestorage platforms, but instead stored on the school's server or school Google Drive.

Any security breaches or attempts, loss of equipment and any unauthorized use or suspected misuse ofIT must be immediately reported to the IT Manager.

Assessing Risks

The school will take all reasonable securities to prevent access to inappropriate material.

However, due to the international scale and Internet connection, it is not possible to guarantee that unsuitable material will never appear on a school computer.

The school cannot accept responsibility for the material accessed by the student, or any consequencesof Internet access.

The school will audit ICT use to establish if the e-safety policy is adequate and that theimplementation of the e-safety policy is appropriate.

Risk mitigation strategies will include preemptive measures such as simulated phishing exercises and regular audits of online platforms used by the school. A dedicated team will be formed to analyze and address any potential risks to online safety.

The school will collaborate with external e-safety experts and organizations to conduct regular training sessions, policy audits, and updates. This partnership ensures the policy remains aligned with international e-safety standards and best practices.

Handling e-Safety complaints

As with all issues of safety at ES, if a member of staff, a student or a parent has a complaint or concern relating to e-safety, prompt action will be taken to deal with it. Complaints should be addressed to the IT manager in the first instance, who will liaise with the senior leadership team andundertake an investigation were appropriate.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the IT manager.

Any complaint about staff misuse must be referred to the Director.

Complaints and concerns of a child protection nature must be dealt with in accordance with schoolchild protection procedures.

Students and parents will be informed of the complaint's procedure.

Complaints related to e-safety will be addressed within 5 working days, with updates provided to the complainant throughout the process. Unresolved issues may be escalated to the Senior Leadership Team for further review.

Communication of Policy

- Students

  Rules for Internet access will be posted in all networked rooms. Students will be informed that Internet use will be monitored.

  A student-led 'Digital Ambassadors' team will be established to promote e-safety, responsible digital behavior, and peer-to-peer support in navigating online environments.

- Staff

  All staff will be given the school e-Safety Policy and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user.

- Parents

  Parents' attention will be drawn to the school e-Safety Policy in Technology Handbook forParents and Students.

Online and Blended Learning (In Case of Need)

Online and blended learning have become integral components of modern education, offering flexibility and continuity in teaching and learning. These approaches ensure uninterrupted education during unforeseen circumstances, such as school closures, while also providing innovative opportunities to enhance the learning experience.

Purpose and Objectives

- The primary goal of online and blended learning is to maintain high-quality education and support student wellbeing, regardless of the learning environment.
- The school emphasizes leveraging technology to complement traditional teaching methods, making education more accessible, interactive, and personalized.

Structure and Expectations

1. **Behavioral Expectations**:
    - Students will be guided on digital etiquette, including appropriate camera use, virtual backgrounds, and microphone discipline.
    - Behavioral expectations and rules for online learning will be clearly communicated to ensure a respectful and productive environment.
2. **Teacher Responsibilities**:
    - Teachers will manage online learning environments, maintaining control over participants, shared content, and interactions.
    - Training will be provided to equip teachers with strategies to engage students, manage disruptions, and monitor participation.
3. **Secure Learning Environment**:
    - All online sessions will use secure meeting links, and teacher-controlled access will be mandatory.
    - Privacy and security protocols, including the use of school-approved platforms, will be strictly followed.
    - Only school-approved platforms will be used for online learning to ensure security and consistency.
4. **Supporting Wellbeing and Engagement**
    - The school recognizes the unique challenges of remote learning and commits to:
        - Balancing screen time with offline activities to prevent fatigue.
        - Providing resources to support mental health and wellbeing.
        - Ensuring timely and constructive feedback to keep students motivated and engaged.
5. **Integration with Regular Curriculum**
    - Online and blended learning will complement in-person classes by offering additional resources, such as recorded lessons, virtual discussions, and interactive assignments.
    - Teachers will align online content with curriculum objectives, ensuring consistency across all learning environments.

Digital Wellbeing

The school will promote digital wellbeing by organizing workshops on managing screen time, recognizing signs of online fatigue, and taking digital breaks. A Digital Wellbeing Committee will oversee these initiatives.

The school is committed to reducing its environmental footprint by promoting the use of digital platforms to minimize paper usage and adopting energy-efficient technologies.

E-Safety Training

Mandatory e-safety training sessions will be conducted annually for staff, with tailored workshops for students and parents to address the latest online safety challenges.

Monitoring and Evaluation

An e-safety evaluation framework will be established, with periodic surveys to assess the policy's effectiveness. Annual reports will highlight achievements, challenges, and areas for improvement.

A feedback mechanism will be established, allowing staff, students, and parents to share their experiences and suggestions regarding the implementation of the e-safety policy. This feedback will inform annual reviews to ensure continuous improvement.

Assessment and Feedback

Providing timely and helpful feedback is a cornerstone of good teaching and learning, and whilst this may be more challenging with online learning, teachers will endeavor to provide regular feedback to learners on pieces of work that they are required to submit.

To maintain academic integrity during online assessments, students will use secure proctoring tools approved by the school. Feedback will be provided through encrypted school platforms to ensure privacy and data security.

Bibliography

International Society for Technology in Education (ISTE). (2021). *Digital Citizenship in Schools: Addressing Online Safety and Responsible Technology Use*. Eugene, OR: ISTE. Available at https://www.iste.org

European Commission. (2021). *EU Guidelines on Children's Online Safety: Protecting Young Digital Citizens*. Brussels: European Union Publications. Retrieved from https://ec.europa.eu/digital-education-action-plan

Common Sense Media. (2020). *Digital Citizenship Curriculum: Tools for Online Safety and Privacy Awareness*. San Francisco: Common Sense Media. Available at https://www.commonsense.org/education

UNESCO. (2020). *Ensuring Online Safety and Digital Well-being for Students*. Paris: UNESCO Publishing. Retrieved from https://unesdoc.unesco.org

Childnet International. (2021). *Online Safety for Schools: Practical Advice and Resources*. London: Childnet. Available at https://www.childnet.com

Microsoft Education. (2021). *Creating a Safer Digital Environment: Tools and Resources for Schools*. Redmond, WA: Microsoft. Retrieved from https://www.microsoft.com/en-us/education

Google for Education. (2022). *Building a Safe and Inclusive Digital Learning Environment*. Mountain View, CA: Google LLC. Available at https://edu.google.com