European School LTD
შპს ევროპული სკოლა

School e-Safety Policy

Review Frequency: Annual
Prepared by: Head of the Department of Innovative Technologies, ITManager
Written in: September 2018
Last review date: November 2021
Last reviewed by: The Department of Innovative Technologies

Sophio Bazadze
Director

შპს "ევროპული სკოლა" საქართველო
GEORGIA
"EUROPEAN SCHOOL"
Ltd
205172917

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.

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, educationalmaterials 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.

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 email on @europeanschool.ge and@americanhighschool.ge server
- 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 theIT manager, who is responsible for school e-safety.

Students should be taught how to research information in the internet and how to validate it beforeaccepting 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 specificpermission.

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.

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.

Publishing Students' Images and Work

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

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

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

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

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, studentsshould contact the e-Safety Officer for assistance.

Security strategies will be discussed with the School Governance.

Protecting Personal Data

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

Data storage and processing

The school takes compliance with Data Protection legislation very seriously. Please refer to the DataProtection 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 encryptedbefore 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 andrequired 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 thatunsuitable 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.

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.

Communication of Policy

- Students

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

- Staff

All staff will be given the school e-Safety Policy and its importance explained. Staff should beaware 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

Online and blended learning may be necessitated by unforeseen issues, such as the global situation of COVID-19, or may become an ongoing part of teaching and learning at European School.

The goal of online and blended learning is to ensure learning continues in the event of school closure. The goal is to carry on learning, but not necessarily replicate a traditional school day as per the timetable. Maintaining high levels of wellbeing and high-quality learning provides additional complexities when students and teachers are working in online and blended environments. Teaching and learning which operates in isolation using innovative technologies come with inherent difficulties in managing student behaviour and meeting learning and engagement goals.

Teachers have control over the online and blended learning environments. This process includes control over who is present, who can speak, what is being shown and shared etc.

Teachers will know to engage in online teaching and learning practices.

All students are to have the behavioural expectations of online learning made clear to them.

Safeguarding during a school closure/partial closure

In the event of a school closure, students, parents, carers and teachers are reminded that the school's Child Protection and Safeguarding Policy still applies to all interactions between students and teachers. Parents need to provide the individual pieces of equipment for their child/children and involvement of student/students. Within the framework of blended learning, the administration should ensure that the IT infrastructure is maintained accordingly

Online Learning

Academic subject areas may also arrange for teaching, teachers to deliver content in a 'live' manner (either by text or audio and/or visual means). This will be carried out with the blended learning approach of online lessons.

Learners will be provided with a school email address to avoid any issues regarding General Data Protection Regulation (GDPR). There will be no expectation for parents/carers or learners to provide their email addresses for use.

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.