Technology Handbook for Parents and Students

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

Technology Handbook for Parents and Students

Introduction

Purpose of the Handbook

The **Technology Handbook for Parents and Students** is designed to provide a comprehensive guide to the technology resources, policies, and best practices within our school. It aims to ensure that parents and students understand their roles and responsibilities in effectively and responsibly using these tools to enhance learning and communication. The handbook also serves as a resource for troubleshooting, accessing support, and staying informed about the latest updates in our technology environment.

This document outlines:

- The key systems and platforms students and parents will use.
- Guidelines for the safe and effective use of technology.
- Policies to ensure data protection and privacy.
- Expectations for behavior when using school-provided or personal devices.

By adhering to the policies in this handbook, we create a secure, collaborative, and enriching digital environments for all.

Review and Update Frequency

This handbook is reviewed and updated annually to reflect the evolving technological landscape, policy changes, and feedback from the school community. Updates are prepared by the **Digital Transformation Permanent Committee** and reviewed by senior leadership.

The last update to this handbook was completed in **November 2024**, and the next scheduled review will occur in **November 2025**.

For questions or suggestions regarding this handbook, please contact the **Digital Transformation Permanent Committee** at digitaltransformation@europeanschool.ge.

ManageBac, Edupage, and QuickSchools

Overview

ManageBac, Edupage, and QuickSchools are the key curriculum management systems used by our school to facilitate communication, manage coursework, and track academic progress. Each platform is tailored to specific programs:

- **ManageBac**: Used by International Baccalaureate (IB) students.
- **Edupage**: Designed for the Georgian National Program.
- **QuickSchools**: Dedicated to the American School of Advanced Studies (ASAS) program.

These platforms provide:

- Access to curriculum details, including unit plans and resources.
- Real-time updates on courses, teachers, and student calendars.
- A record of academic progress, attendance, and homework schedules.
- An online grade book with summative assessments, semester grades, and reports.

- Communication tools for messaging between students, teachers, and parents.

Key Expectations:

Students are expected to regularly access their accounts to check for updates, assignment deadlines, and communication from teachers. Parents can log in to monitor their child's academic progress, view homework calendars, and download reports.

Troubleshooting Common Issues

To ensure uninterrupted access to these platforms, follow these steps for resolving common issues:

1. **Forgot Password**
    - Contact the respective support team.
2. **Access Problems**
    - Verify your internet connection and ensure your browser is updated to the latest version.
    - Clear your browser cache and cookies if the platform is not loading correctly.
3. **Technical Support Contacts**

    For unresolved issues, please contact the appropriate support team within the school for assistance with ManageBac, Edupage, or QuickSchools.

User Guides

To help students and parents navigate these platforms effectively, the school has developed comprehensive user guides, available on the school's website. These guides include:

- Step-by-step instructions on accessing and using the platforms.
- Visual aids like screenshots and video tutorials for common tasks such as:
    - Viewing homework and deadlines.
    - Downloading grades and reports.
    - Sending messages to teachers.

Accessing User Guides:

- Visit the "For Parents" section on the websites of all three school programs.
- Printed copies of user guides are available upon request at the school's main office.

For additional support, the school also conducts training sessions at the beginning of the academic year to familiarize new students and parents with the systems.

Google Email, Apps, and Online Storage

The school provides each student with a personal Google email account under the @europeanschool.ge domain. These accounts are available to all classes and serve as essential communication tools for students and teachers, seamlessly integrating with various Google applications frequently used in the classroom.

Key Features

- **Unlimited Cloud Storage:** The **@europeanschool.ge** account provides students with unlimited online storage, enabling them to save documents, projects, and other learning materials securely

in the cloud. This allows students to access their files from any location or device with internet access.

- **Collaboration Tools:** Students can use Google Workspace applications, such as Google Docs, Sheets, and Slides, to collaborate on assignments and projects in real-time.
- **Streamlined Communication:** Gmail facilitates efficient communication between students, teachers, and staff, fostering a collaborative learning environment.

Students are strongly encouraged to store their learning materials using their Google accounts to ensure their work is secure and easily accessible.

Digital Citizenship Training

To promote safe and responsible use of these tools, the school provides **Digital Citizenship** training to all students before they begin using their Google accounts. This training aligns with the **ISTE (International Society for Technology in Education) Standards for Students**, which empower students to take ownership of their learning in a safe, legal, and ethical manner.

Key principles of the Digital Citizenship standard include:

- **Digital Identity and Reputation Management:**
  Students learn to build and maintain a positive digital identity and understand the long-term impact of their online actions.
- **Safe, Legal, and Ethical Behavior:**
  Students practice responsible use of technology, including online interactions and the use of networked devices.
- **Respect for Intellectual Property:**
  Students gain an understanding of copyright laws and learn how to share and use content legally and ethically.
- **Personal Data Management:**
  Students develop strategies to protect their privacy, secure their personal information, and recognize how data-collection technologies track online navigation.

Responsibilities of Students

Students are expected to exhibit the same appropriate behavior online as they do in the classroom or on school grounds. This includes:

- Using school-owned Google accounts and the internet exclusively for school-related tasks.
- Avoiding unauthorized activities such as gaming, inappropriate browsing, or sharing offensive content.
- Taking responsibility for maintaining the security of their Google account, including safeguarding their password.

Responsibilities of Teachers

All teachers are provided with a Google account under the **@europeanschool.ge** or **@americanhighschool.ge** domains, granting them the same unlimited storage and access to Google tools. Teachers use these accounts to:

- Store and share educational resources with students and colleagues.
- Facilitate e-learning activities and manage assignments through Google Classroom and other applications.

- Provide feedback and support to students using Google Workspace tools.

By leveraging these tools, teachers ensure that learning resources are accessible and organized, supporting a seamless integration of technology into the curriculum.

Additional Notes

- Both students and teachers are advised to regularly back up critical files stored in their Google accounts.
- For support with Google accounts or Google Workspace tools, contact the school's IT team at **itsupport@europeanschool.ge**.

Bring Your Own Device: Laptops and Tablets

The school has implemented a **Bring Your Own Device (BYOD)** program for students in Secondary and High School (Grades 6 to 12). This program allows students to bring their personal laptops or tablets to school to enhance their learning experience through research, note-taking, and e-learning classroom activities.

Device Readiness and Use

- Students must ensure their devices are **fully charged** before arriving at school, as charging during school hours is not permitted due to limited access to power outlets.
- Devices should be used strictly for **educational purposes** during class and only as instructed by the teacher.

Important Guidelines

- Students are responsible for the maintenance and security of their devices. The school is not liable for loss, theft, or damage.
- Devices must have basic productivity software installed, including Google Workspace tools, to support classroom activities.

By adhering to these guidelines, the BYOD program aims to provide students with a more flexible and technology-enhanced learning environment.

Information Storage and Maintenance

As students increasingly store their learning materials in electronic files, it is their responsibility to ensure the **secure storage** and proper organization of their work.

Key Responsibilities for Students

- **Backup Systems:**
  Students must set up reliable backup solutions, such as using external hard drives, USB drives, or cloud-based services like Google Drive, to prevent data loss.
- **Device Maintenance:**

  Both hardware and software must be well-maintained. Regular software updates, including operating system and antivirus software, should be performed to ensure devices operate efficiently and securely.

Important Notes

- The school **cannot retrieve lost data** from students' personal devices.

- The school does not provide repair services for personal laptops, tablets, or other devices. Students should consult professional repair services if needed.

By adopting these practices, students can minimize the risk of losing important academic materials and ensure uninterrupted learning.

Internet Access

The school provides **high-speed LAN and wireless internet access** in both buildings to support students' learning and research needs. Each student is issued a unique password to connect their personal devices, such as laptops or tablets, as well as to access school computers on the LAN.

Student Privileges and Guidelines

- **Connecting Personal Devices:**
  Students may connect their devices to the school network using their assigned credentials.
- **Using School Computers:**
  Students are permitted to use school computers as per the **Acceptable Use Policy** and must follow school regulations.
- **Device Use in Classrooms:**
  Personal devices may only be used in classrooms with the teacher's permission for activities such as note-taking or research.
- **Software Requirements:**
  Students can use their own software, provided it is compatible with the educational requirements specified by the teacher.

Acceptable Use Policy Reminder

All internet use must align with the school's **Acceptable Use Policy**, which prohibits accessing inappropriate content, using the internet for non-educational purposes during class, or engaging in disruptive online activities.

Security

The school is committed to providing a **safe and secure environment** for students and teachers. Several measures are in place to safeguard both people and property:

Measures in Place

1. **Lockers:**
   Each student is provided with a locker and is strongly encouraged to store their electronic devices securely when not in use.
2. **Security Cameras:**
   All school buildings are equipped with security cameras to monitor public areas and enhance safety.
3. **Secure Pass System:**
   External doors are protected by a pass system to control access and ensure the safety of everyone on campus.

Student Responsibility

While the school takes extensive precautions, students who bring personal devices such as laptops or tablets do so **at their own risk**. The school **cannot be held responsible** for any costs associated with the loss, theft, or damage of personal items on campus.

Recommendations for Students:

- Keep devices in lockers when not in use.
- Label devices with your name to ensure they are easily identifiable.
- Use protective cases for devices to minimize the risk of damage.

By adhering to these guidelines, students can make the most of the school's resources while maintaining the security of their personal belongings.

Use of IT

All students who access the internet or use personal devices at school must agree to and comply with the **European School Acceptable Use of ICT Policy**. This policy outlines the responsibilities of students and parents in ensuring the safe and appropriate use of the school's digital technologies and resources.

Purpose of the Acceptable Use Policy

The policy aims to:

1. Foster responsible and appropriate use of digital technologies.
2. Promote positive attitudes and behaviors that protect students, the European School community, and the school's IT resources.
3. Ensure students understand their digital responsibilities both within and beyond the school environment.

Policy Structure

The policy consists of two key components:

1. **Acceptable Use of IT at ES:**

   This section provides specific rules for using the school's IT systems and resources, including:

   - Proper use of shared technology in classrooms.
   - Secure and respectful behavior when accessing school networks and systems.

2. **Guidelines for the Use of Digital Technologies:**

   This section offers general advice for responsible digital technology use, covering:

   - Social media etiquette.
   - Online behavior both inside and outside of the school environment.

Technologies and Resources Covered

The policy applies to the following resources:

- **Personal Digital Learning Resources Provided by ES:** Includes devices, software, and tools issued to students.

- **Shared Classroom Technology:** Such as laptops, workstations, interactive whiteboards, and projectors.
- **Local and Wireless Network Resources:** Use of the school's LAN and Wi-Fi networks.
- **Cloud-Based Systems:** Includes Google Workspace and other online tools provided by the school.
- **Other Digital Resources:** Use of third-party educational platforms or applications.
- **Data Protection and Security Measures:** Ensuring secure handling of data and adherence to the school's privacy protocols.

Parental Involvement

Parents play a vital role in supporting their children's responsible use of IT:

- **Read the Policy Together:** Parents are encouraged to review the Acceptable Use Policy with their children to ensure they fully understand the expectations.
- **Discuss Digital Responsibilities:** Help your child develop good habits for using digital technologies safely and effectively.

By agreeing to the policy, parents and students commit to fostering a safe, respectful, and productive digital learning environment at European School.

Electronic Devices

During school activities, students are permitted to use **electronic devices** only for **educational purposes** and with prior approval from the teacher in charge. Non-educational electronic devices, such as portable music players or gaming devices, are generally not allowed during lessons.

Usage Guidelines

- **Educational Use:** Devices such as laptops or tablets may be used in class strictly for learning activities, as directed by the teacher.
- **Personal Use During Breaks:**
    - Students may use portable music devices during lunchtime, break time, or study periods, provided this does not compromise their safety or disrupt others.
    - In the library or study rooms, music can only be played with headphones and at a volume that does not disturb others.

Storage of Devices

At all other times, personal electronic devices must be kept securely in **lockers** or **bags** when not in use.

Responsibility

The school is **not liable** for the loss, theft, or damage of personal electronic equipment. Students are encouraged to:

- Clearly label their devices with their name for easy identification.
- Use protective cases to prevent damage.

By following these guidelines, students can balance the use of electronic devices while maintaining a focus on learning and ensuring a respectful environment for others.

Shared Classroom Technology

The school provides a wide range of classroom technology resources to support the curriculum and enhance the learning experience. These resources include:

- Laptops and workstations.
- Interactive whiteboards and projectors.
- Specialized hardware and tools for various subjects.

Student Responsibilities

Students are expected to:

1. **Treat Technology with Care and Respect:**
    - Avoid mishandling or misusing any classroom technology.
    - Ensure devices and equipment remain in good condition during and after use.
2. **Report Damage Immediately:**
    - Any damage or malfunction must be reported promptly to the class teacher to ensure timely repairs and continued availability for other users.
3. **Avoid Unauthorized Modifications:**
    - Students must not change physical connections or alter software configurations on any device without explicit permission from the teacher.
    - If permission is granted, the device must be returned to its original settings after use.

Best Practices for Shared Technology Use

To ensure the continued functionality and availability of shared technology, students should:

- Log out of personal accounts after use to maintain privacy.
- Handle all equipment gently, especially portable devices like laptops.
- Avoid placing food or drinks near any technology to prevent accidental damage.

By following these guidelines, students contribute to a respectful, efficient, and effective use of the school's shared technology resources.

Local and Wireless Network Resources

The school provides students with access to both the **Local Area Network (LAN)** and the **wireless network** to support their educational activities. By connecting to these networks, students acknowledge that they have read and understood the school's **Acceptable Use of ICT Policy** and agree to adhere to its guidelines.

Usage Guidelines

- **Permitted Use:**

  Students may use the network to access educational resources, complete assignments, and participate in online learning activities.

- **Prohibited Actions:**

- Students must not install, or attempt to install, any unauthorized software on school-owned devices or network systems.
- Security settings and permissions for any school devices or networks must not be altered under any circumstances.

Network Security and Responsibility

- The school actively monitors network activity to ensure compliance with security protocols and to protect users from potential threats.
- Students are responsible for ensuring their personal devices are free from malware and viruses before connecting to the school network.

By following these rules, students help maintain a secure and reliable network environment for all users.

Cloud-Based Systems and Resources Provided by ES

ES provides a wide and constantly evolving collection of online systems and resources, many of which require users to log in with personal account names and passwords. These account details must be carefully protected and should never be shared with or disclosed to anyone.

It is crucial to ensure that you log out properly from any secure system you access through a shared ES device. If you discover that another user has left their personal account open, please log out of the account immediately or inform a teacher or the IT support team.

Sending an inappropriate message from another user's email account is a serious violation of the **Acceptable Use of ICT Policy** and will be subject to disciplinary action.

Do not synchronize personal data from an online system onto an ES shared device to prevent unauthorized access or data loss.

If you suspect that one of your personal accounts has been compromised, notify the IT team immediately for assistance.

Use of Other Digital Resources

The following guidelines govern the use of the internet and other digital resources provided by the school, focusing on areas that may have serious, and potentially legal, implications for students and the school.

Students Must:

- **Avoid Inappropriate Content:**
  Students must not deliberately access, transmit, copy, or create material that is inappropriate. This includes, but is not limited to, content that is pornographic, threatening, rude, discriminatory, or intended to harass others.
- **Respect Intellectual Property:**
  Students must respect and protect the intellectual property of others. This includes refraining from making or distributing illegal copies of music, games, movies, or other copyrighted materials.
- **Abstain from Criminal Activities:**
  Digital resources must not be used to further any criminal acts.

- **Avoid Sending Unsolicited Communications:**
  Students must not use digital resources to send spam, chain letters, or other unsolicited mass communications.
- **Restrict Commercial Activities:**
  Buying, selling, advertising, or conducting business through the school's ISP resources or systems is prohibited unless explicitly approved as part of a school project.
- **Avoid Plagiarism:**
  All work submitted as coursework or assignments must include proper acknowledgment of sources. Plagiarism of any kind is strictly prohibited.

By adhering to these guidelines, students contribute to a responsible and ethical use of digital resources, maintaining the integrity and safety of the school's digital environment.

Data Protection and Security

Students must adhere to the following guidelines to ensure the security and integrity of the school's digital systems and resources:

- **Use Assigned Accounts Only:**
  Students must use only their assigned accounts to access ES systems or resources.
- **Respect Authorization Boundaries:**
  Students must not attempt to view, use, or copy passwords, data, or networks for which they do not have explicit authorization.
- **Avoid Unauthorized Software:**
  The installation of unauthorized software on any school device or system is strictly prohibited.
- **Report Issues Promptly:**
  Any suspected security violations or vulnerabilities should be reported immediately to the IT team to ensure prompt resolution.
- **Follow Network Security Practices:**
  Students must comply with all network security guidelines and protocols, as posted or communicated by the school.
- **Refrain from Tampering with Data:**
  Students must not delete, edit, or move data or resources that do not belong to them.

By following these rules, students help maintain a secure, efficient, and respectful digital environment for all users.

Privacy and E-safety

Students are expected to adhere to the following guidelines to ensure their own safety and the privacy of others when engaging with digital tools and platforms:

- **Use Approved Communication Channels:**

  Communicate with ES staff only through assigned **Google Apps email addresses**, school-approved management systems, or other authorized channels.
- **Respect Privacy:**

Protect the privacy of others and yourself by refraining from posting or distributing private or sensitive information online. This includes personal details, photos, or videos without explicit consent.

- **Report Concerns Promptly:**

  If a student feels threatened, uncomfortable, or encounters inappropriate behavior online, they must report the incident immediately to a teacher or the school's IT team.

By following these principles, students contribute to a respectful and safe digital environment that aligns with the school's e-safety standards.

Supervision and Monitoring of IT Resources

To maintain a secure and effective digital environment, the school and IT administrators actively monitor the use of IT resources. This monitoring ensures compliance with the school's mission and promotes the safety, discipline, and well-being of the community.

Monitoring Practices

- The school reserves the right to **examine, use, and disclose any data** found on its networks or information systems to:
  - Safeguard the health, safety, discipline, or security of any student or staff member.
  - Protect school property and resources.
- User accounts and internet activity are subject to monitoring, with logs maintained to identify and address inappropriate activities.

Responsibilities and Consequences

- Students are expected to use IT resources thoughtfully and responsibly, adhering to the school's Acceptable Use Policy.
- Information gathered during monitoring may be used in disciplinary actions to address violations.
- When necessary, evidence of illegal activities will be provided to law enforcement agencies, in compliance with **Georgian and international laws**.

By following these guidelines, students contribute to a secure and respectful digital environment while protecting the integrity of the school's IT resources.

Consequences for Violation

Violations of the school's IT rules and policies may result in disciplinary action. Depending on the severity of the violation, consequences may include:

- **Loss of Privileges:**
  Students may lose access to the school's IT resources, including internet, school accounts, and devices, either temporarily or permanently.
- **Additional Disciplinary Measures:**
  Further disciplinary actions may be taken in accordance with the school's code of conduct by school administration.

- **Reporting to Authorities:**
  In cases involving illegal activities, such as hacking, data theft, or accessing prohibited content, the school may report the incident to law enforcement authorities in compliance with **Georgian and international laws**.

Students are encouraged to use IT resources responsibly to avoid these consequences and maintain a secure and productive learning environment.

Bibliography

International Society for Technology in Education (ISTE). (2021). *Essential Technology Skills for Students and Parents: Guidelines for Digital Learning Success*. Eugene, OR: ISTE. Retrieved from https://www.iste.org

European Commission. (2022). *Digital Competence Framework for Educators (DigCompEdu)*. Brussels: European Union Publications. Available at https://ec.europa.eu/education

Common Sense Media. (2020). *A Parent's Guide to Digital Learning: Best Practices and Safety Tips*. San Francisco: Common Sense Media. Available at https://www.commonsense.org/education

Department for Education (DfE). (2021). *Online Learning: Guidance for Parents and Students*. London: Department for Education. Available at https://www.gov.uk/government/publications/online-learning-guidance-for-schools

Google for Education. (2022). *Tools and Resources for Digital Learning: Supporting Parents and Students in Online Environments*. Mountain View, CA: Google LLC. Retrieved from https://edu.google.com