

# European Azerbaijan School



## Technology Acceptable Use Policy for staff and students

Revised by the Director, Principals, Deputy Principals, IB coords, Teachers 11/03/2026

## **Introduction and Aims**

At The European Azerbaijan School (EAS), the welfare and well-being of all students is our highest priority. This Technology Acceptable Use Policy is designed to ensure that every user can benefit from modern communication technologies while following safe, responsible, and appropriate practices. The policy provides clear and consistent guidelines that promote the positive use of digital tools and prevent misuse.

EAS recognizes that devices such as mobile phones, tablets, laptops, and smartwatches can serve as valuable communication and learning tools. However, the advanced features available on many devices may lead to distraction, reduce productivity, or create opportunities for inappropriate use. Because it is often difficult to determine how a device is being used at any moment, this policy applies broadly to all personal communication and digital devices brought onto school premises.

When reading this policy, particular attention should be given to the terms “Student” and “User.” The term “User” refers to all members of the school community who access or interact with the school’s technology infrastructure. This includes students, parents, and employees. In addition, independent contractors, consultants, volunteers, temporary staff, visiting scholars, interns and campus visitors are all subject to the same rules and expectations outlined in this policy.

## **Code of Conduct**

The school promotes a Code of Conduct to support a cooperative and respectful working and learning environment. All users are expected to work collaboratively, demonstrate high ethical standards, and respect one another. This approach helps build strong morale, a sense of responsibility, and a positive school culture that supports productivity and learning.

The aim of this code is to ensure that all users:

- Have a clear understanding of what constitutes misuse of technology and digital resources.
- Know how to minimize risks when using digital tools, online platforms, and school systems.
- Avoid placing themselves in situations that could be misinterpreted or lead to allegations of inappropriate conduct.
- Understand the importance of maintaining professional boundaries when communicating or interacting through digital technologies.
- Take personal responsibility for monitoring and managing their own behavior when using school technology.
- Recognize the importance of promptly reporting concerns, misuse, or inappropriate behavior.
- Bullying, harassment, or intimidation using digital platforms is strictly prohibited.
- Users must not share information on behalf of the school without authorization from school leadership.
- The school name, brand, and logo may not be used for personal, commercial, or unofficial purposes without explicit permission.

Failure to follow this Code of Conduct may result in disciplinary action in accordance with school policies.

### **Personal and Business Mobiles – Staff**

- Staff are not permitted to make/receive calls/texts during contact time with students.
- Staff are only permitted to use their mobile phones during break and lunch time in a space where students are not present.
- Emergency contact should be made via the school office mobile phones and/or via landlines located in the primary or secondary campus, whenever possible.
- Mobile phones must be kept on silent mode or switched off and stored out of sight during class time.
- Mobile phones must not be used in any area where students are present (e.g., classrooms, corridors, playgrounds).
- Staff must security protect access to their phone.
- Should there be exceptional circumstances then staff can ask permission from the Principal
- Staff are not at any time permitted to use recording equipment on their mobile phones, for example: to take recordings of students/teachers, or to share images. Legitimate recordings and photographs should be captured using school equipment.
- Staff must report any concerning or inappropriate mobile phone use by colleagues to the Principal.
- Mobile phones should not be used to contact parents during school time.
- Staff are not permitted to use their phones for sharing non-related content via WhatsApp or other social media.

### **Personal Mobiles/Devices – Students**

We recognize that mobile phones are a normal part of everyday life and that they may help students feel safe and connected. However, they can also distract from learning, disrupt lessons, and provide opportunities for misuse, including bullying or the inappropriate sharing of content. For these reasons, and in accordance with our Yondr system, the following rules apply:

- Students are not permitted to access or use their mobile phones during school hours.
- All students must place their mobile phones into a Yondr pouch upon entering the school. The pouch will be locked for the entire school day and opened only at the designated unlocking stations when students leave the campus.
- Any mobile phone brought to school must be placed in the Yondr pouch without exception.
- If a student attempts to unlock, tamper with, or misuse a Yondr pouch, the phone will be confiscated, and disciplinary action will follow.
- Smartwatches or any wearable devices with communication or internet capabilities are not permitted and are treated as mobile phones under this policy.
- Unauthorized use of a mobile phone, including attempts to access it while the pouch is locked, will be recorded and may result in additional sanctions.
- In exceptional situations requiring phone use (e.g., medical need), parents may request approval from the school administration.

Internet and network access provided by the school is not a public service. Therefore, the school reserves the right to monitor all use of its computer systems, networks, internet access, and related digital services. The school may take appropriate action against any user who fails to comply with The European Azerbaijan School's policies and guidelines.

### **Parents' communication with teachers**

EAS uses Managebac as the main school administration and communication system.

- Parents should use Managebac or email to contact teachers.
- WhatsApp groups are used only for Advisors and Homeroom teachers to share urgent information.
- WhatsApp groups should be used only for clarifications and important information.
- Managebac in Primary is used to share class activities, news, and post related to teaching and learning
- Parents should contact teachers only after school for urgent communications.
- Parents should contact the school's office to take appointments

### **Cyber Security**

The European Azerbaijan School is committed to maintaining a secure digital environment that protects students, staff, and the school's technological infrastructure. To achieve this, the school implements multiple cyber-security measures, including firewalls, web-filtering systems, secure authentication processes, and continuous network monitoring. These safeguards are designed to minimize risk and ensure that users access only appropriate and authorized online content.

While the school takes all reasonable precautions to filter and monitor internet activity, no system can guarantee complete protection from unsuitable or harmful material. Therefore, The European Azerbaijan School cannot accept liability for any content that may be encountered, nor for any consequences resulting from internet use on school devices or networks.

Users are expected to act responsibly at all times and to follow all cyber-security guidelines outlined in this policy. Any suspicious activity, security incident, or attempted breach must be reported immediately to the ICT Department or to Principals.

### **Prohibited Cyber Activities**

To protect the integrity of the school's ICT systems and ensure a safe online environment, the following activities are strictly prohibited:

- Attempting to bypass, disable, or tamper with firewalls, filters or any other security controls.
- Attempting to encrypt, hide, or disguise internet activity using VPNs, proxies, or similar tools without explicit permission.
- Accessing websites, servers, or digital resources that are blocked, restricted, or inappropriate.

- Downloading or installing unauthorized software, applications, or browser extensions on school devices.
- Engaging in hacking, phishing, password-guessing, or any attempt to gain unauthorized access to systems, accounts, or data.
- Sharing personal login credentials or using another person's account for any purpose.
- Connecting unauthorized personal devices to the school network without approval from the ICT Department.
- Creating, storing, or sharing malicious files such as viruses, spyware, or harmful scripts.
- Using school systems to engage in online bullying, harassment, or the distribution of harmful or inappropriate content.

## **Personal Security**

To protect the safety, privacy, and professional boundaries of all members of The European Azerbaijan School community, the following rules apply:

- Students and teachers must not connect, “friend,” follow, or otherwise engage with each other on personal social networking platforms. Professional boundaries must be maintained at all times.
- Users must ensure that any videos, photographs, or documents shared through Google Workspace (Google Apps) are shared only through secure links and are not publicly searchable through search engines or open platforms.
- All digital communication between users must remain professional, respectful, and focused on academic or school-related matters.
- Personal contact information should never be shared between students and staff. Communication should occur only through approved school channels.
- Users must not post or share any school-related information, images, or videos on personal social media without explicit permission from school leadership.
- Users must report any concerns relating to digital safety, privacy violations, or inappropriate online behavior to Principals immediately.

## **Cyber Bullying**

The European Azerbaijan School is committed to providing a safe and respectful digital environment for all users. Any form of cyber bullying, online harassment, or misuse of technology is strictly prohibited. The following rules apply:

- Users must not use The European Azerbaijan School's technology resources to create, post, or share any content that is defamatory, inaccurate, abusive, profane, threatening, offensive, discriminatory, or illegal.
- Users must not re-post, forward, or distribute private messages. Confidential or personal information about others must never be shared online.
- Students and teachers are prohibited from posting or uploading any videos, photographs, or audio recordings taken on school premises to public platforms.

- Users must not use the internet or any digital communication tool to bully, intimidate, or harass others, whether directly or indirectly. This includes name-calling, spreading rumors, exclusion, impersonation, or using inappropriate or harmful language.
- Any form of online harassment, including messages sent through social media, email, messaging apps, gaming platforms, or anonymous services, is strictly forbidden.
- Cyber bullying incidents will be treated with the same seriousness as face-to-face bullying and will result in disciplinary action in accordance with school policy.
- Users are expected to report any online behavior that is concerning, harmful, or violates this policy to a teacher, advisor, school counsellor, or Principals
- The school reserves the right to investigate digital activity conducted on school devices or BYOD devices and using school accounts to ensure the safety and well-being of the community.

### **Computers Used in School**

- Students may use computers or tablets only when a teacher is present and has authorized their use.
- Users must not take screenshots, photographs, or recordings of a teacher's computer screen without explicit permission.
- Users must report any damaged devices, unusual system behavior, or suspected security issues to the ICT Department immediately.
- All activity on school computers may be monitored to ensure safe and responsible use.

### **Digital Accounts**

The European Azerbaijan School provides all staff and students with digital accounts to support teaching, learning, and communication. The proper use and security of these accounts are essential to maintaining a safe and effective digital environment.

- Teachers and staff are provided with both Google Workspace and Office 365 accounts for academic and administrative purposes.
- All teachers are required to use Two-Factor Authentication (2FA) on their Google Workspace and Office 365 accounts.
- Teachers are not permitted to disable, remove, or bypass 2FA under any circumstances.
- 2FA must remain active at all times to ensure the security of school data, email accounts, and digital resources.
- Any issues with authentication, lost devices, or difficulties accessing accounts must be reported immediately to the IT Department, who will assist with secure recovery.
- Attempts to disable or avoid 2FA will be treated as a violation of the school's ICT Security Policy.
- Students are provided with Google Workspace (Google Suite) accounts only, for academic use.
- All digital accounts are personal, private, and non-transferable. Users must not share their passwords or allow anyone else to access their account.
- If a user believes that their account has been accessed by someone else, they must change their password immediately and inform the IT Department without delay.
- Users must log out of shared or public devices after use.

- Students must ensure that files shared through Google Workspace are set to “Share with link only” or other privacy-appropriate settings.
- If students are unsure how to adjust privacy settings, they should request assistance from the IT Department.
- Students’ Google Workspace accounts are to be used exclusively for academic purposes (classwork, homework, communication with teachers, school projects).
- Staff must use their school-provided accounts for professional and school-related communication only.
- Users must always communicate using respectful, appropriate, and academic-focused language.
- Users must not use school digital accounts to create, share, or access inappropriate, harmful, or unrelated personal content.
- School accounts must not be used to register for personal services, games, or non-academic websites.

### **Monitoring and Misconduct**

The ICT Department, with the Director’s authorization, may monitor any school-issued digital account and its content whenever necessary to ensure compliance with school policies and to protect the security of the school’s digital environment.

If any misconduct, misuse, or policy violation is detected in relation to the use of a digital account, the school reserves the right to suspend or restrict the account immediately. Further disciplinary actions may be taken in accordance with school regulations and the severity of the violation.

### **Saving Work**

- Students should use their Google Drive account to save their work. This is the only way to ensure that work is backed up and secure.
- Students are encouraged to have a personal backup of their work; this is best facilitated by using Google Drive to store work, but a USB drive may also be used for this purpose. Google Drive has unlimited free storage.

### **Bring Your Own Device (BYOD)**

- Approved devices for student use must be in silent mode while on the school campus unless otherwise allowed by a teacher. Headphones may be used with teacher permission.
- Devices may not be used without permission on assignments, quizzes, or tests.
- Devices may not be used during lessons for non-instructional purposes (such as making personal phone calls and text messaging).
- Devices may only be used to access resources on internet sites that are relevant to the classroom curriculum.
- Devices may not be used during breaks and after school.

### **Sanctions Against Misconduct or Inappropriate Use**

The European Azerbaijan School will address any incidents of misconduct, inappropriate use of technology, or willful damage on a case-by-case basis, taking into account the severity and context of the violation.

With the authorization of the CEO, the ICT Department reserves the right to access, review, and monitor any digital accounts or digital content operated through The European Azerbaijan School's systems. This includes school-issued email accounts, cloud storage, documents, communication tools, and any other managed digital services.

If any form of misuse or policy violation is detected, the school may impose one or more of the following sanctions:

- Suspension or restriction of the user's digital account
- Temporary or permanent removal of access to ICT resources
- Confiscation of devices where necessary
- Administrative or disciplinary action in accordance with school regulations
- Notification of parents/guardians in the case of student misconduct
- Financial compensation for intentional damage to school equipment
- Referral for further action depending on the seriousness of the breach

#### Profile Photos

- All teachers and students must maintain a clear, appropriate profile photo on their school-issued digital accounts (Google Workspace, Office 365, Managebac or etc).
- Users are not permitted to remove or replace the required profile photo.
- Profile photos must follow school guidelines and may be updated only with approval from the ICT Department.

#### School-Issued Devices

- Users must not place stickers, decorations, writing, or adhesives on any school-issued equipment, including laptops, iPads, or accessories.
- Users must not remove, cover, or tamper with school labels, asset tags, barcodes, or identification stickers placed by the ICT Department.
- Any damaged, missing, or defaced school label will result in a report and possible sanctions, including financial responsibility for repairs or replacement.

#### Printer Usage

- Teachers and staff are permitted to use school printers for academic, administrative, and school-related tasks.
- Students are not permitted to use school printers unless specifically authorised by a teacher or the ICT Department for an academic requirement.
- Users must print only essential documents and avoid unnecessary printing to support sustainability and responsible resource use.
- Users must not attempt to alter printer settings, connect personal devices to printers, or install unauthorised drivers or software.
- Any printer issues, errors, or malfunctions must be reported to the ICT Department immediately.
- Abuse of printing privileges may result in restricted access or disciplinary measures.

#### **ICT Policy Acknowledgement**



**Name:** \_\_\_\_\_

**Position:** \_\_\_\_\_

I understand and acknowledge that all text, photo, video, and audio information related to The European Azerbaijan School (including the school, staff, students, and parents) is the property of EAS. This information must remain confidential, may be used only for official purposes, and must not be shared, transferred, or disclosed outside EAS without proper authorization.

I understand that any intentional or unintentional disclosure, unauthorized access, sharing, or careless handling of this information constitutes a breach of EAS regulations. I acknowledge that EAS reserves the right to take appropriate legal or administrative action resulting from such a data breach.

**Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_