Baleares International College
Sa Porrassa
an Orbital Education School

Orbitaled

E-Safety and Acceptable Use of IT Policy

Approved by:	Alison Colwell, Principal
Last reviewed on:	March 2024
Next review due by:	March 2027

E-Safety and Acceptable Use of IT Policy

Scope
This policy is applicable to all members of the school community—staff, students, parents, visitors, and community users—who access school digital technology systems both within and outside school premises. The school will address e-safety incidents and inform parents about inappropriate online behaviors occurring outside of school.

Roles and Responsibilities
- **Regional Head of Schools (RHoS)**: Represents the Board of Directors in approving and reviewing the policy. Receives regular updates on online safety incidents.
- **Principal**: Oversees the overall safety (including online) of the school community, delegates day-to-day online safety tasks to the Deputy Designated Safeguarding Lead (DDSL), ensures training for staff, and maintains a monitoring system to provide a safety net and support for colleagues.
- **Online Safety Lead (DDSL)**: Manages daily online safety issues, reviews policies, provides staff training, liaises with municipal and technical staff, and logs incidents for ongoing improvements. Reports to the Principal.
- **ICT Manager/Technical Staff**: Ensure secure infrastructure, adhere to online safety technical standards, enforce password protection, update monitoring tools, and oversee network usage to prevent misuse.

Parents
Parents are vital in teaching their children to use the internet and mobile devices safely. The school encourages parents to support its online safety initiatives and adhere to guidelines regarding:
- Use of digital and video images from school events.
- Access to the parent sections of the school website, learning platforms and, online student records.

Recognising that many parents may not be fully aware of online safety risks, the school commits to enhancing parental understanding through:
- Educational activities incorporated into the curriculum.
- Communications such as letters, newsletters, and updates via the school's website and Learning Platform.
- Parent meetings and participation in events like Safer Internet Day. Directing parents to informative resources such as www.saferinternet.org.uk and www.childnet.com/parents-and-carers.

Education and Training

Online safety is integral to all curriculum areas, ensuring that staff consistently emphasize its importance. The curriculum will include comprehensive and progressive online safety education, integrated into subjects like Computing and PHSE, and revisited regularly. Key messages will be reinforced through assemblies and pastoral activities. Students will learn to critically assess and verify online content in every lesson and practice safe, responsible internet use inside and outside of school. Additionally, staff will model exemplary behavior in their digital technology use and undertake regular online safety training with a focus on recognising and handling online safety incidents. New staff will receive online safety training (EduCare - Online Safety for International Schools) as part of their induction programme.

Technical – Infrastructure, Equipment, Filtering, and Monitoring

The school is committed to maintaining a secure network and infrastructure. We ensure:

- Implementation of robust security measures to protect servers, firewalls, routers, wireless systems, workstations, and mobile devices from unauthorised access. All systems undergo regular security testing and are equipped with up-to-date antivirus software.
- Establishment of protocols for granting temporary system access to guests such as trainee teachers, supply teachers, and visitors.
- Secure encryption or protection of personal data before it is transmitted over the internet or removed from school premises.

The school ensures a secure network environment with up-to-date protections against threats, regular security checks, and controlled access for guests. Personal data is securely encrypted when transferred over the internet or off-site.

Mobile Device Usage Policy

Mobile devices offer valuable tools in educational settings, facilitating activities such as recording work, planning via electronic calendars, researching, emailing work, and using digital and online learning resources. However, their use must be regulated to ensure safety and appropriateness:

- **During School Hours**: Staff are prohibited from using mobile phones during lessons or when on duty. Mobile phones should not be used near students.
- **Photography and Recording**: Taking photos or recording videos of students, staff, or school property requires express permission from a senior staff member. Additionally, consent from the subject or the subject's parent must be obtained before capturing images or videos.
- **Sharing Images:** Posting or sharing images of students, staff, or the school on public or private websites, or transferring these images to others, is strictly forbidden without the Principal's explicit approval.

Use of Digital and Video Images Policy

Digital imaging technology enhances learning by allowing staff and students to quickly use images they have recorded or downloaded. However, there are risks associated with posting these images online.

Guidelines for Use:

- **Parental Consent**: Written permission must be obtained from parents before publishing photographs of students on the school website, social media, or in the local press.
- **Usage by Staff and Volunteers**: Digital or video images taken to support educational goals must adhere to school policies on sharing, distribution, and publication. Such images must be captured using school equipment only; personal devices are not permitted for this purpose.
- **Publication Standards**: Images including students posted on the school website or other platforms will be carefully chosen and adhere to best practice guidelines for safe use. Students' full names will not be associated with any photographs published online to protect their privacy and security.

Data Protection Policy
General Principles:
Personal data at Baleares International College, Sa Porrassa is managed in compliance with current data protection laws. This includes:

- **Minimal Collection**: Only the necessary personal data required for school operations is collected and retained only for its intended purpose and duration.
- **Accuracy**: Data must be accurate and kept up-to-date, with inaccuracies corrected promptly.
- **Lawful Processing:** The basis for processing personal data, including consent where applicable, is clearly documented and communicated via a privacy notice.
- **Secure Deletion**: Once data is no longer needed or has been transferred, it is securely deleted in accordance with school policy.

Communication Technologies:

- **Email Communications**: The school provides a monitored and secure email service for staff and student use. All communications should occur over this service, particularly when in school or accessing school systems remotely.
- **Reporting Inappropriate Communications**: Any inappropriate, offensive, discriminatory, threatening, or bullying communications must be reported to the Principal immediately without responding.
- **Professional Digital Communications**: All digital interactions between staff, students, and parents (via email, social media, chat, blogs, VLE, etc.) must maintain a professional tone and content and occur only on officially monitored school systems. Personal contact details must not be used for these communications.
- **Online Safety Education**: Students are educated about the risks associated with sharing personal details online and are taught strategies to handle inappropriate communications effectively.

Social Media - Protecting Professional Identity

Social media is a valuable tool for learning and communication in schools. However, its use must be managed responsibly to maintain a safe learning environment.

Key Guidelines:

- Duty of Care Schools are responsible for ensuring the online interactions of their employees do not harm others or the school's reputation.
- Professional Conduct: Staff must avoid harassment, bullying, discrimination, or defamation on social media. Such actions can make the school liable for damages.
- Preventive Measures: Schools must implement and enforce policies to prevent foreseeable harm related to social media use by staff.

These guidelines help safeguard the professional identities of school staff and uphold the school's duty of care in digital interactions.

Social Media Policy for School Staff
General Guidelines:

- **No References**: Staff must not mention students, parents, or fellow staff members on social media.
- **Avoid Personal Discussions**: Do not engage in online discussions about personal matters involving the school community.
- **No Attribution of Personal Opinions**: Staff should not attribute personal opinions to the school or Orbital Education.

Official Social Media Accounts:

- **Approval Process**: All posts must be approved by the Principal before publication.
- **Administration and Monitoring**: At least two staff members should oversee the administration and monitoring of these accounts.
- **Handling Abuse**: Implement systems for reporting and addressing abuse or misuse, aligned with school disciplinary procedures.

Monitoring Public Social Media:

- **Proactive Monitoring**: Regularly check the internet for public posts about the school.
- **Response Protocol**: Respond to social media comments about the school according to established policies.

Compliance Checks:

- **Regular Reviews**: The Head of Admissions will routinely check the school's professional social media use to ensure compliance with policies.

Incident Response for Misuse of Online Services
This policy provides guidance for staff on how to handle incidents involving misuse of online services, ensuring a secure response to activities that may be illegal or inappropriate.

Handling Illegal Incidents
If you suspect a website contains child abuse images or any other illegal activity, immediately refer to the Principal and Designated Safeguarding Lead (DSL).

School Actions and Sanctions
If you suspect illegal activity, such as child abuse images, on a website, immediately report to the Principal and the Designated Safeguarding Lead (DSL).

Acceptable Use Policy

Purpose:
This policy governs the use of electronic devices to ensure a safe and secure educational environment, enhance learning, and promote digital citizenship.

Definitions:
- **Electronic Devices:** This includes any device capable of taking photos, recording audio or video, storing/transmitting/receiving messages or images, or connecting to the Internet wirelessly. Examples include desktops, laptops, tablets, smartphones, e-readers, and other similar technologies.
- **Digital Citizenship:** The standards of responsible and ethical use of technology, covering areas like digital literacy, ethics, etiquette, and online safety.
- **User:** Anyone authorised to use electronic devices, including students, parents, staff, volunteers, visitors, contractors, and service providers' personnel.

1. Authorised Use of Electronic Devices
Electronic devices are permitted on school premises for educational and administrative use only, within approved areas and times, under staff supervision. Authorised users must:
- Adhere to the school Code of Conduct when using electronic devices.
- Follow staff guidelines for electronic device use on school property or during school activities.
- Obtain consent and authorisation from school personnel before taking photos or making audio/video recordings for educational purposes.
- Connect to the school network via approved infrastructure only.

2. Responsibilities
All users must:
- Register their electronic device with the school and submit a signed Electronic Devices Use Agreement before connecting to the school network.
- Use electronic devices in line with school policies and procedures.
- Care for, secure, and store their devices properly.
- Keep account details, login names, passwords, and lock codes private to ensure device and data security.
- Maintain a safe and productive learning environment when using devices.
- Practise good digital citizenship.

Teachers' Responsibilities:
- Create equal learning opportunities using electronic devices when relevant to the curriculum.

- Decide when students may use school or personal electronic devices for educational purposes.
- Supervise students' use of electronic devices.
- Address disciplinary issues arising from inappropriate use of electronic devices.
- Communicate with senior, parents, and students regarding any violations of school policy related to electronic device use.

Students' Responsibilities

- Use electronic devices for educational purposes only, in approved areas, and under staff supervision.
- Perform virus and malware scans on their devices.
- Report any inappropriate use of electronic devices to a teacher or senior leaders immediately.
- Ensure their devices are fully charged before bringing them to school.
- Continue learning by alternative methods if their electronic device malfunctions.

Parents' Responsibilities

- Assist their children in properly caring for, maintaining, securing, storing, and transporting their electronic devices.
- Help their children protect the privacy of their device accounts, login details, and lock codes.
- Label their child's electronic device and record its make, model, and serial number or install tracking software.
- Obtain theft or hazard insurance for the electronic device.
- Encourage adherence to school policies and the practice of good digital citizenship.
- Contact the school office to communicate with their child during school hours, avoiding digital communication that is not related to education.
- Take full responsibility for their child's use of non-school internet connections, like 3G/4G networks.

3. Unauthorised Use of Electronic Devices

The following activities are prohibited when using electronic devices:

- Using devices in private areas such as changing rooms or restrooms.
- Bypassing the school's network to use external wireless services.
- Downloading non-educational files.
- Engaging in activities unrelated to education, such as gaming, watching videos, social media, listening to music, texting, or making personal calls.
- Cheating on assignments or tests.
- Accessing or distributing confidential information.
- Using photos, audio, or video recordings for non-school-related purposes.
- Gaining unauthorised access to or tampering with data.
- Participating in cyberbullying or using technology to harm others.
- Introducing viruses or harmful software.
- Committing any act that violates federal, provincial, or municipal laws.
- Violating copyright or plagiarism laws.
- Using school network resources for commercial activities or political campaigning.

4. Consequences: Remedial and Disciplinary Action

Individuals who violate this policy will face consequences aligned with the school's Code of Conduct. Depending on the specific case, these may include:

- Temporary confiscation of the device.
- Inspection of the device to find evidence of misuse.
- Restrictions, suspension, or revocation of access to personal and school technology resources.
- Disciplinary actions, which may include dismissal.
- Legal action and potential prosecution by appropriate authorities.

5. Liability

Users who bring electronic devices to school are solely responsible for their care and usage. Devices are brought at the user's own risk. The school and its personnel will not be liable for any loss, damage, misuse, or theft of student-owned electronic devices, whether on school premises, in school vehicles, during transport, or at school-sponsored events. Additionally, the school is not responsible for any issues that arise from running specific software or connecting to the school network on these devices.

6. Technical Support

School personnel will not provide technical support, troubleshooting, or repair services for user-owned electronic devices.

Review and Compliance

The effectiveness of this policy is regularly monitored by the Principal and Orbital Education and is reviewed by the Principal every three years, next due **March 2027**, to ensure it meets the needs of the school community and complies with statutory requirements.