Baleares International College
Mallorca
an Orbital Education School

Orbitaled

Online Safety Policy

BIC Sa Porrassa

and

BIC San Agustí

Approved by:	Group Head of IT Operations Lee Collins Director of Education Michael Clack Group Head of HR Andy Edgar	**Date:** 31/07/2025
Last reviewed on:	July 2025	
Next review due by:	July 2026	

Development / Monitoring / Review of this Policy

This policy has been developed by a working group comprising:

- Principal / Senior Leaders
- Online Safety Officer / Coordinator
- Staff (Teachers, Support Staff, Technical Staff)
- Regional Head of Schools / Board
- Parents
- Student Representatives

Schedule for Development / Monitoring / Review:

- Approval: By the Board on 31/07/2025
- Monitoring: By the Senior Leadership Team at least annually
- Reporting: Annually to the Regional Head of Schools and the Board, with immediate reporting for serious incidents
- Review: Annually or as needed based on new developments or incidents by RHoS on behalf of the board

Scope of the Policy

This policy applies to all members of the school community (staff, students, volunteers, parents, visitors, community users) who use school digital technology systems and networks, both in and out of the school.

Under the UK Education and Inspections Act 2006, Principals are reasonably empowered to regulate student behaviour off-site, and staff may impose disciplinary measures for misconduct, including online bullying linked to school membership. The Education Act 2011 (Section 24b) extends these powers to include searching electronic devices and deleting data, the keeping children safe in education statutory guidance (KCSIE) 2025 also outlines new definitions of online risks. Principals must ensure similar authority exists under host country legislation. Actions must align with the school's published Behaviour Policy. The school will address such incidents through its Online Safety, Behaviour, and Anti-Bullying policies, and will inform parents when inappropriate online behaviour outside school is identified.

Types of risks

- It is essential that children are safeguarded from potentially harmful and inappropriate online material.
- The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:
- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism,

radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are

AI Content

The expectation is that

- Users are effectively and reliably prevented from generating or accessing harmful and inappropriate content
- Filtering standards are maintained effectively throughout the duration of a conversation or interaction with a user
- Filtering will be adjusted based on different levels of risk, age, appropriateness and the user's needs - for example users with special educational needs and disabilities (SEND)
- Multimodal content is effectively moderated, including detecting and filtering prohibited content across multiple languages, images, common misspellings and abbreviations
- **Full content moderation capabilities are maintained regardless of the device used, including bring your own device (BYOD) and smartphones when accessing products via an educational institutional account**
- Content is moderated based on an appropriate contextual understanding of the conversation, ensuring that generated content is sensitive to the context
- Filtering should be updated in response to new or emerging types of harmful content refer to the School AI policy for further information.

Roles and Responsibilities

All roles including external guests and must read and accept the acceptable use policy before accessing and using the schools' local and online systems and networks. The following online safety responsibilities apply to roles in the group as detailed below:

Board of Directors

- Approval of the Online safety policy
- Reviewing the effectiveness of the policy based on feedback from the RHoS

Regional Head of Schools (RHoS)

- Take on the role of Online Safety Operational board member which includes:
    - Regular meeting with the Online Safety Co-ordinator/ Designated Safeguarding Lead/Principal
    - Approves and reviews any changes to the policy
    - Monitors online safety incidents and reports
    - Reporting to the board of Incidents

Principal and Senior Leaders

- Ensure the safety of the school community
- Make sure there is comparable authority/ power under the legislation of the host country
- Ensure that there is a system in place for monitoring, reporting, and receiving incident reports from the online safety officer / Lead
- Delegate day-to-day online safety responsibilities to the Online Safety Officer / Designated Safeguarding Lead (DSL)
- Ensure all staff receive suitable training

Online Safety Officer / Lead (DSL or DDSL)

- Leads the Online Safety Group
- Manages day to day online safety incidents, and maintains the Incident log *(a sample of one can be provided if required)*
- Reviews process and policy and suggests improvements or non-compliance to the leadership team
- Provides training and advice to all staff
- Liaises with technical staff and external authorities

Network /IT Manager / Technical Staff

- Stays up to date on online safety training and policy
- Ensures the physical access security of the school's technical infrastructure is in place
- Implements and monitors online safety measures and ensures they are up to date including firewall, anti-virus protection
- Ensures all technology related to online access is protected in line with any local regulations and the online safety policy and baselines

- Ensures any contracted 3rd party suppliers follow the online safety measures and are fully aware of the schools' process before working in the school *(this must be done during induction /onboarding at contract start)*
- Ensures that any messaging and collaboration platforms are monitored for misuse and in the event of an incident, report to the Online Safety Officer and senior leadership team for investigation
- Ensures that physical access to IT systems is restricted to the appropriate level and that users have clearly defined access rights including, online and removable storage, staff and student data systems, organisational data and internet access.
- Ensures that all students and staff are provided with a username and password that meets security standards outlined in the password policy. And that no generic user accounts are in use in any school systems.
- Makes sure that all master admin usernames and passwords are stored in an encrypted vault of which the principal has access to in case of emergencies for business continuity.
- Ensures that all software licenses are up to date and cover the number of seats /devices in use in the school.
- Ensures that all internet access is filtered to the appropriate age and role level in the school and that the firewall and security gateways are up to date and that the security controls reflect the safeguarding controls outlined in the safeguarding controls policy.
- Support Online safety Officer in ensuring that a system is in place to monitor, record and report on online safety incidents.
- Ensures that the Acceptable use policy is available to Staff, Students, Parents and 3rd party collaborators and is enforced **before** access is granted to school systems and networks.
- Conduct a cyber risk assessment annually and review every term
- Develop and implement a plan to back up your data and review this every year
- Report all cyber attacks

Utilise the UK Department for Education's filtering and monitoring standards or similar local standards for reference in what to control.

Teaching and Support Staff

- Stay updated on online safety matters
- Embed online safety in the curriculum
- Ensure they have read the Online safety policy and Acceptable Use Policy
- Monitor and guide students' use of digital technologies
- In the event of observing any misuse, report to the Online Safety Officer and senior leadership team for investigation

- Ensure that all communications with students and parents are carried out on Official School systems and conversations are always of a professional nature
- Ensure Students understand the Online safety policy and how to avoid plagiarism and copyright infringement
- In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies regarding these devices

Students

- Use school digital technology systems responsibly following the acceptable use policy
- Report misuse or inappropriate materials
- Understand the online safety policy and acceptable use policy.
- Follow guidance on good practice, taking images safely, appropriate mobile phone use, and an understanding of online bullying.

Parents

- Support the school's online safety policies
- Monitor their children's online activities
- Understand the importance of good online safety and what it looks like
    - Digital photo and video images at and around school events
    - Safe access and sharing guidance on parents' sections of learning platforms and online student records
    - Good personal device use (where in place in the school)

Education and Training

While regulation and technical measures are important, educating students to act responsibly online is essential. Online safety and digital literacy are key parts of the school's provision, helping students recognise risks and build resilience. Online safety should be integrated across the curriculum, with staff reinforcing key messages. The curriculum for online safety should be broad, age-appropriate, and offer progression through creative learning opportunities, tailored to the school's structure and student age groups.

Students Education

To ensure a consistent and effective approach to online safety, the school will implement the following measures:

- **Curriculum Delivery:** A structured online safety curriculum will be delivered through Computing, PSHE, and other relevant subjects, with regular reinforcement.
- **Whole-School Messaging:** Key online safety messages will be embedded in assemblies, tutorials, and pastoral programmes.
- **Critical Thinking:** Students will be taught to critically evaluate online content and verify its accuracy.
- **Digital Responsibility:** Lessons will include guidance on acknowledging sources and respecting copyright.
- **Resilience to Radicalisation:** Students will be supported in developing resilience through safe discussions of controversial topics and understanding civic participation as opposed to extremism.
- **Acceptable Use:** Students will be educated on the importance of the Acceptable Use Policy and encouraged to use technology responsibly in and out of school.
- **Staff Role Modelling:** Staff will model appropriate use of digital technologies, the internet, and mobile devices.
- **Safe Browsing Practices:** In pre-planned internet use, students will be directed to vetted websites, and procedures will be in place to manage exposure to unsuitable content.
- **Monitoring:** When students have open internet access, staff will actively monitor their activity.
- **Access to Restricted Content:** For legitimate educational purposes (e.g. research on racism, drugs, discrimination), staff may request temporary access to blocked sites. Such requests must be auditable and justified, using a template available from Orbital.

Parent Education and Engagement

Parents play a vital role in guiding and monitoring their children's online behaviour, yet many may be unaware of the risks or how to respond to online safety concerns. To support parents, the school will provide regular information and raise awareness through:

- Curriculum-linked activities
- Communications (e.g. letters, newsletters, website, learning platform)
- Parent sessions and events
- Campaigns such as Safer Internet Day
- Signposting to trusted resources (e.g. saferinternet.org.uk, childnet.com)
- Provided with information and resources to support online safety at home

Staff / Volunteers education and engagement

- Receive regular formal, audited Online Safety training as part of their CPD and mandatory training plan
- New staff trained as part of their induction, completed within the first 3 weeks
- Be asked to review and formally agree with Online safety policies and other related policies as part of INSET days

Regional Head of Schools and Board

Participate in regular formal, audited Online Safety training as part of their CPD and mandatory training plan

Dealing with Incidents of Misuse

This section will cover the steps required to deal with incidents and aims to ensure:

- Clear procedures for handling incidents are followed
- Immediate reporting of serious incidents to the appropriate authorities is carried out

Incidents

When investigating incidents, you must:

- Involve at least two senior staff to ensure accountability.
- Use a designated computer not accessible to students; this device may be required by police.
- Ensure investigators have monitored and recorded internet access.
- Maintain a timeline of events for potential police reporting.
- Record URLs and describe concerning content; capture and store screenshots if needed (excluding child abuse images).
- After investigation, determine if the concern is valid and take appropriate action:
    - Internal disciplinary measures
    - Referral to the Regional Head of Schools or relevant authorities
    - Police involvement

Mandatory Police Referral

The following incidents must be reported to the police without exception:

- Child abuse imagery
- Grooming behaviour
- Sending obscene materials to a child

- Breaches of the Obscene Publications Act
- Criminally racist content
- Promotion of terrorism or extremism
- Other criminal activities

Safeguarding Measures

- Isolate the computer to preserve evidence and avoid the chance of tampering.
- Follow all steps in a chronological log to create a clear evidence trail for safeguarding and legal purposes.
- Retain the completed investigation form /log for reference.

Actions and Sanctions

It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. The following actions and sanctions are suggested for staff and student incidents.

Staff Incidents and Actions:

Scenario	Action 1	Action 2	Action 3	Action 4	Action 5
Unauthorised downloading or uploading of files	Warning	disciplinary action	suspension	refer to Principal	refer to RHoS / HR
Continued infringements of the above, following previous warnings or sanctions	Disciplinary action	suspension	refer to Principal	refer to RHoS / HR	
Breaching copyright or licensing regulations	Warning	disciplinary action	suspension	refer to Principal	refer to RHoS / HR
Deliberately accessing or trying to access offensive or pornographic material	Suspension	refer to Principal	refer to RHoS / HR	refer to Police	
Accidentally accessing offensive or pornographic material and failing to report the incident	Warning	disciplinary action	refer to Principal	refer to RHoS / HR	
Using proxy sites or other means to subvert the school's filtering system	Disciplinary action	suspension	refer to Principal	refer to RHoS / HR	

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	Disciplinary action	suspension	refer to Principal	refer to RHoS / HR	
Actions which could compromise the staff member's professional standing	Disciplinary action	suspension	refer to Principal	refer to RHoS / HR	
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students	Disciplinary action	suspension	refer to Principal	refer to RHoS / HR	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	Disciplinary action	suspension	refer to Principal	refer to RHoS / HR	refer to Police
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	Disciplinary action	suspension	refer to Principal	refer to RHoS / HR	refer to Police
Deliberate actions to breach data protection or network security rules	Disciplinary action	suspension	refer to Principal	refer to RHoS / HR	refer to Police
Careless use of personal data e.g. holding or transferring data in an insecure manner	Warning	disciplinary action	refer to Principal	refer to RHoS / HR	
Allowing others to access school network by sharing usernames and passwords or attempting to access or accessing the school network, using another person's account	Disciplinary action	suspension	refer to Principal	refer to RHoS / HR	
Inappropriate personal use of the internet / social media / personal email	Warning	disciplinary action	refer to Principal	refer to RHoS / HR	
Deliberately accessing or trying to access material that could be considered illegal	Suspension	refer to Principal	refer to RHoS / HR	**refer to Police**	

Student Incidents and Actions

Scenario	Action 1	Action 2	Action 3	Action 4	Action 5
Unauthorised downloading or uploading of files	Warning	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
Continued infringements of the above, following previous warnings or sanctions	Further sanction e.g. detention / exclusion	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
Breaching copyright or licensing regulations	Warning	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
Deliberately accessing or trying to access offensive or pornographic material	Suspension	removal of network / internet access rights	refer to Principal	inform parents / carers	refer to Police
Accidentally accessing offensive or pornographic material and failing to report the incident	Warning	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
Using proxy sites or other means to subvert the school's filtering system	Disciplinary action	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	Disciplinary action	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	Disciplinary action	removal of network / internet access rights	refer to Principal	inform parents / carers	refer to Police
Corrupting or destroying the data of other users	Disciplinary action	removal of network / internet access rights	refer to Principal	inform parents / carers	refer to Police
Deliberate actions to breach data protection or network security rules	Disciplinary action	removal of network / internet access rights	refer to Principal	inform parents / carers	refer to Police
Careless use of personal data e.g. holding or transferring data in an insecure manner	Warning	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network,	Disciplinary action	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–

using another person's account					
Inappropriate personal use of the internet / social media / personal email	Warning	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
Deliberately accessing or trying to access material that could be considered illegal	Suspension	removal of network / internet access rights	refer to Principal	inform parents / carers	**refer to Police**