E-Safety Policy

A. SCOPE

The school is committed to promoting and safeguarding the welfare of all students, for which an effective online safety strategy is essential.

The growth of electronic media in daily life and the increasing variety of devices generate various risks for children and young people, such as access to inappropriate content, the bypassing of age restrictions to communicate with strangers, grooming and digital sexual abuse, the unauthorized disclosure of personal information, online gambling or indebtedness, cyberbullying, and the inappropriate use of Artificial Intelligence.
In light of this environment, the fundamental objectives of our strategy are:

- Protecting the entire school community from illegal, inappropriate, or harmful content or contact.
- Educating on responsible, ethical, and safe access to and use of technology.
- Establishing effective mechanisms to identify, intervene in, and escalate incidents in a timely manner.

For the purposes of this policy, the school adopts a broad vision of the concept of technology, encompassing networks, platforms, digital tools, and devices used to view, generate, or exchange information. Its provisions apply to all members of the school community—staff, contractors, volunteers, students, parents, and visitors—who use technology, networks (including institutional Wi-Fi networks from personal BYOD devices), platforms, and institutional school accounts, whether they are inside or outside the premises, or whose digital activity affects the welfare of others, personal data protection, or institutional reputation.

This directive forms part of the institutional regulatory framework and is cross-functionally complemented by the Staff Code of Conduct, the Acceptable Use Policy (Student Handbook), the Anti-Bullying Policy, the IT infrastructure and social media policy, as well as the rest of the school regulations. To learn in detail about comprehensive safeguarding and case response protocols, the General Child Protection and Safeguarding Policy can be consulted on our institutional website.

B. ROLES AND RESPONSIBILITIES

1. General Management and ISP

General Management has overall responsibility for safeguarding mechanisms within the school, including the online safety strategy and the use of technology. General Management must ensure that all those with leadership and management responsibilities actively promote the welfare of students. The adoption of this policy forms part of this responsibility. General Management will conduct an annual review of safeguarding procedures and their

implementation, including the effectiveness of this and related policies, based on the established objectives.

2. General Management and Leadership Team

General Management has executive responsibility for the safety and welfare of members of the school community. Designated Safeguarding Leads (DSLs) are members of the Leadership Team with responsibility for child protection and welfare. Their responsibility includes managing safeguarding incidents related to the use of technology, in accordance with the School's Safeguarding Policy. The Leadership Team will work with the IT Coordinator and the IT Department to monitor technology use and practices within the school, and evaluate potential improvements to ensure the digital welfare of students. The Leadership Team will regularly review the Technology Incident Log. DSLs will regularly update the leadership team on the operation of safeguarding mechanisms, including online safety practices.

3. IT Coordination

The IT Coordinator, along with their team, is responsible for the operation and effectiveness of the school's filtering system in order to prevent access to material that poses risks, including extremist or terrorist material. The IT Coordinator must ensure that:

- The school's technological infrastructure is secure and not vulnerable to misuse or attacks.
- Only authenticated and authorized users can access school technology.
- The filtering system is current, effective, and regularly updated.
- The risk of students or staff bypassing the protection systems implemented by the school is minimized.
- The use of technology is regularly monitored to ensure compliance with this policy.
- Monitoring software is kept up to date and allows tracking of email and internet use.

The IT Coordinator will report to the Leadership Team on the operation of technological systems and will escalate any concerns immediately. Likewise, they will maintain the Technology Incident Log and report any risk situation to the DSL, in accordance with the Safeguarding Policy.

4. All Staff

Staff must act as role models for responsible conduct in the use of technology and share safe school policies and practices with students. Staff must report any concern related to student welfare or safety, in accordance with the Safeguarding Policy.

5. Parents

The role of parents is key to ensuring that students understand how to stay safe in the digital environment. The school expects parents to:

- Support the implementation of this policy and report concerns.
- Talk with their children about the use of networks, devices, and digital media.
- Encourage their children to report situations of cyberbullying or digital risk.

C. EDUCATION AND TRAINING

1. Students

Safe use of technology is an integral part of the IT curriculum. Students receive guidance on the safe use of the internet, social media, and mobile devices. In Early Years, technology is integrated through exploration, play, and recognition of its use in everyday contexts both at home and at school. Likewise, digital safety messages are reinforced through classes, assemblies, and tutoring sessions to teach:

- Risks associated with technology use.
- Validation of digital information.
- Identification of suspicious behaviors, harassment, radicalization, and extremism.
- Concept and effects of cyberbullying.
- Consequences of negative online behavior.

2. Staff

The school provides training to ensure that staff understand digital risks and know how to act during incidents. Induction includes training in the Digital Safety Policy, Code of Conduct, Email and Network Policy, and guidelines for the professional use of social media.

3. Parents

Parents are invited to review the Acceptable Use Policy included in the Student Handbook with their children.

D. ACCESS TO SCHOOL TECHNOLOGY

All access requires a personal username and password, which must not be shared. Visitors have a separate Wi-Fi network and controlled access.

E. USE OF MOBILE DEVICES

The school has filtering and monitoring systems; however, it recognizes that mobile data can allow unregulated access. The use of personal devices must have prior authorization.

F. PROCEDURES IN CASE OF MISUSE

All incidents must be reported in accordance with discipline, safeguarding, and conduct policies.

G. MONITORING AND REVIEW

All serious incidents will be recorded and evaluated within digital safety reviews, to improve protection mechanisms.

Prepared by:	Reviewed by:	Authorized by:
ISP • Eustolia Martínez Rodríguez	• Charlotte Crossland • Eustolia Martínez Rodríguez • Amanda Martín del Campo Jensen • Jennifer Barbour Martínez • María José Valencia González	Charlotte Crossland Oct 2026