Online Safety Policy

Approved by: Raúl Fernández Pascual, Principal, Colegio CEDES	**Last reviewed on:** June 2026
Next review due by: June 2027	

1. Purpose

Online Safety is an integral component of safeguarding at Colegio CEDES, helping to protect the school community from risks such as exposure to harmful content, cyberbullying, grooming and radicalisation. This policy helps ensure that students can access the benefits of the internet safely while minimising potential risks and harm.

2. Scope

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

Where the school places students with an alternative provision provider, it continues to be responsible for the safeguarding of those students. An assessment against this policy will be made with the provider, and the school should obtain written confirmation online safety controls are in place.

3. Legislation and Guidance

The Keeping Children Safe In Education (KCSIE) statutory guidance outlines definitions of online risks, including from AI and deepfake technologies. Relevant Spanish legislation includes Organic Law 8/2021 on the Comprehensive Protection of Children and Adolescents against Violence (LOPIVI), Organic Law 3/2018 on Personal Data Protection and Guarantee of Digital Rights (LOPDGDD), Regulation (EU) 2016/679 (GDPR), and Organic Law 2/2006 on Education (LOE), as amended by Organic Law 3/2020 (LOMLOE).

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. In Spain, the relevant framework is provided by Organic Law 2/2006 on Education (LOE), as amended by Organic Law 3/2020 (LOMLOE), Organic Law 8/2021 (LOPIVI), and applicable regional education regulations and school procedures governing student behaviour, safeguarding, online safety and the use of personal electronic devices.

The school will address online misconduct through a range of policies, and will inform parents when inappropriate online behaviour outside school is identified.

3.1 Types of Risks

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, including AI-generated images, audio or video.

Examples include pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, impersonation, misinformation, disinformation (including fake news) and conspiracy theories.

- **Contact:** being subjected to harmful online interaction with other users.

Examples include peer-to-peer pressure, commercial advertising or 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.

Examples include making, sending, receiving or sharing explicit images (both consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), harassment or online bullying

- **Commerce:** risks such as online gambling, inappropriate advertising, phishing or financial scams.

3.2 Inappropriate 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 is regularly updated in response to new or emerging types of harmful content and AI tools users may access.

4. Roles & 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 responsibilities for online safety apply to specific roles:

4.1 School Board

- Approval of the Online Safety Policy
- Review the effectiveness of the policy based on feedback from the RHoS

4.2 Regional Head of Schools (RHOS)

- Act as the Operational Board member responsible for Online Safety, which includes:
- Holding regular meetings with the Online Safety Co-ordinator/Designated Safeguarding Lead/Principal;
- reviewing and approving any changes to the policy;
- monitoring online safety incidents and reports;
- reporting incidents to the Operational Board.

4.3 Principal and Senior Leaders

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

4.4 Online Safety Officer/Designated Safeguarding Lead (or Deputy)

- Lead the Online Safety Group
- Manage day-to-day online safety incidents, and maintains a record of all incidents
- Review process and policy and suggests improvements or non-compliance to the leadership team
- Provide training and advice to all staff
- Liaise with technical staff and external authorities

4.5 Network/It Manager and Technical Staff

- Stay up-to-date with regard to online safety policy, practice and training
- Ensure the physical security of the school's technical infrastructure
- Implement and monitor online safety measures and ensure they are up-to-date, including firewall and anti-virus protection
- Ensure all technology related to online access is protected in line with local regulations, the Online Safety Policy and group baselines
- Ensure any contracted third-party suppliers follow the online safety measures and are fully aware of the schools' processes before working in the school
- Ensure 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
- Ensure that physical access to IT systems is restricted to the appropriate level and that users have clearly defined access rights (this includes online and removable storage, staff and student data systems, organisational data and internet access).
- Ensure 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.
- Ensure that all master admin usernames and passwords are stored in an encrypted vault, and that the Principal has access to this in case of emergencies for business continuity.
- Ensure that all software licenses are up to date and cover the number of users/ devices in use in the school.
- Ensure that all internet access is filtered to the appropriate age and role level in the school, 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 the Online Safety Officer/DSL in ensuring that a system is in place to monitor, record and report online safety incidents.
- Ensure that the Acceptable Use of IT Policy is available to staff, students, parents and third-party collaborators, and is enforced **before** access is granted to school systems and networks.
- Conduct an annual cyber risk assessment, and review this each term
- Develop and implement a plan to back up the school's data and review this each year
- Report all cyber attacks

4.6 Teaching and Support Staff

- Read, understand and comply with the Online Safety and Acceptable Use of IT policies
- Stay updated about online safety matters
- Embed online safety in the curriculum
- Monitor and guide the students' use of digital technologies
- Report any misuse to the Online Safety Officer and senior leadership team for investigation
- Ensure that all communications with students and parents are made using official school systems, and that 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, ensuring processes are in place for dealing with any unsuitable material that is found in internet searches
- monitor and implement current policies regarding devices whenever the use of digital technologies, mobile devices, cameras, etc. is allowed in lessons and other school activities

4.7 Students

- Understand the Online Safety and Acceptable Use of IT policies
- Use school digital technology systems responsibly, following the Acceptable Use of IT Policy
- Report misuse or inappropriate materials
- Follow guidance on good practice, taking images safely, appropriate mobile phone use, and develop an understanding of online bullying

4.8 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, with particular regard to:
- good personal device use
- 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

5. 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.

5.1 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 of IT 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, and may be approved by the Principal, in consultation with the RHoS where necessary.

5.2 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 raise awareness and provide regular information through:

- curriculum-linked activities
- communications (e.g. letters, newsletters, website, learning platform)
- parent sessions, workshops and events
- campaigns (e.g. Safer Internet Day)
- signposting to trusted resources (e.g. saferinternet.org.uk, childnet.com)
- providing information and resources to support online safety at home

5.3 Staff/Volunteers Education and Engagement

- All staff receive regular formal, audited online safety training as part of their CPD and mandatory training plan
- New staff receive online safety training as part of their induction, completed within the first 3 weeks

- All staff review and formally agree with the Online Safety Policy and other related policies as part of start-of-year activities or in-year induction

5.4 Regional Head of Schools (RHOS) and School Board

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

6. Dealing with Incidents of Misuse

This section covers the steps required to deal with incidents and aims to ensure that:

- clear procedures for handling incidents are followed; and
- immediate reporting of serious incidents is made to the appropriate authorities.

6.1 Incidents

When investigating incidents, school leaders will:

- 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 the investigators have monitored and recorded internet access;
- maintain a timeline of events for potential police reporting;
- record URLs and describe concerning content. The capture and storing of screenshots maybe beneficial, but must exclude images of child abuse;

After investigation, the school leaders will determine if the concern is valid and take appropriate action:

- internal disciplinary measures;
- referral to the Regional Head of Schools and/or other relevant authorities;
- police involvement.

6.2 Mandatory Police Referral

Certain 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

6.3 Safeguarding Measures

- The computer used for investigation should be isolated, to preserve evidence and avoid the chance of tampering.
- All steps followed should be recorded in a chronological log to create a clear evidence trail for safeguarding and legal purposes.
- The completed investigation form/log must be retained for reference.

6.4 Actions and Sanctions

It is important that any incidents are dealt with as soon as possible, and in a proportionate manner. It is also important that members of the school community are aware that incidents have been dealt with.

A process flowchart and suggested actions and sanctions for incidents are included in the Appendix.

7. Monitoring and Review

This policy has been developed by a working group comprising:

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

7.1 Schedule for Monitoring, Review and Further Development

- V1 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

following incidents, by RHoS on behalf of the Board

8. Related Policies

This policy should be read in conjunction with the following documents:

- Safeguarding Policy
- Behaviour and Anti-Bullying policies
- Acceptable Use of IT, AI, Password, Social Media and Safeguarding Controls policies
- Keeping Children Safe In Education (KCSIE) 2026

9. Useful References

UK Safer Internet Centre: saferinternet.org.uk - guides and resources

- In particular, the UK Safer Internet Centre has produced a series of webinars for teachers on behalf of the DfE to inform and support schools with their filtering and monitoring responsibilities - Appropriate Filtering and Monitoring

UK government: Education, training and skills - gov.uk

- Filtering and Monitoring Standards
- Cyber security standards for schools and colleges developed to help them improve their resilience against cyber-attacks
- Preventing Bullying (includes cyberbullying)
- Information sharing for people who provide safeguarding services to children

UK Council for Internet Safety: UKCIS

- Sharing nudes and semi-nudes advice for schools and colleges on responding to incidents of consensual and non-consensual sharing of nudes and semi-nudes.

Childnet: Childnet

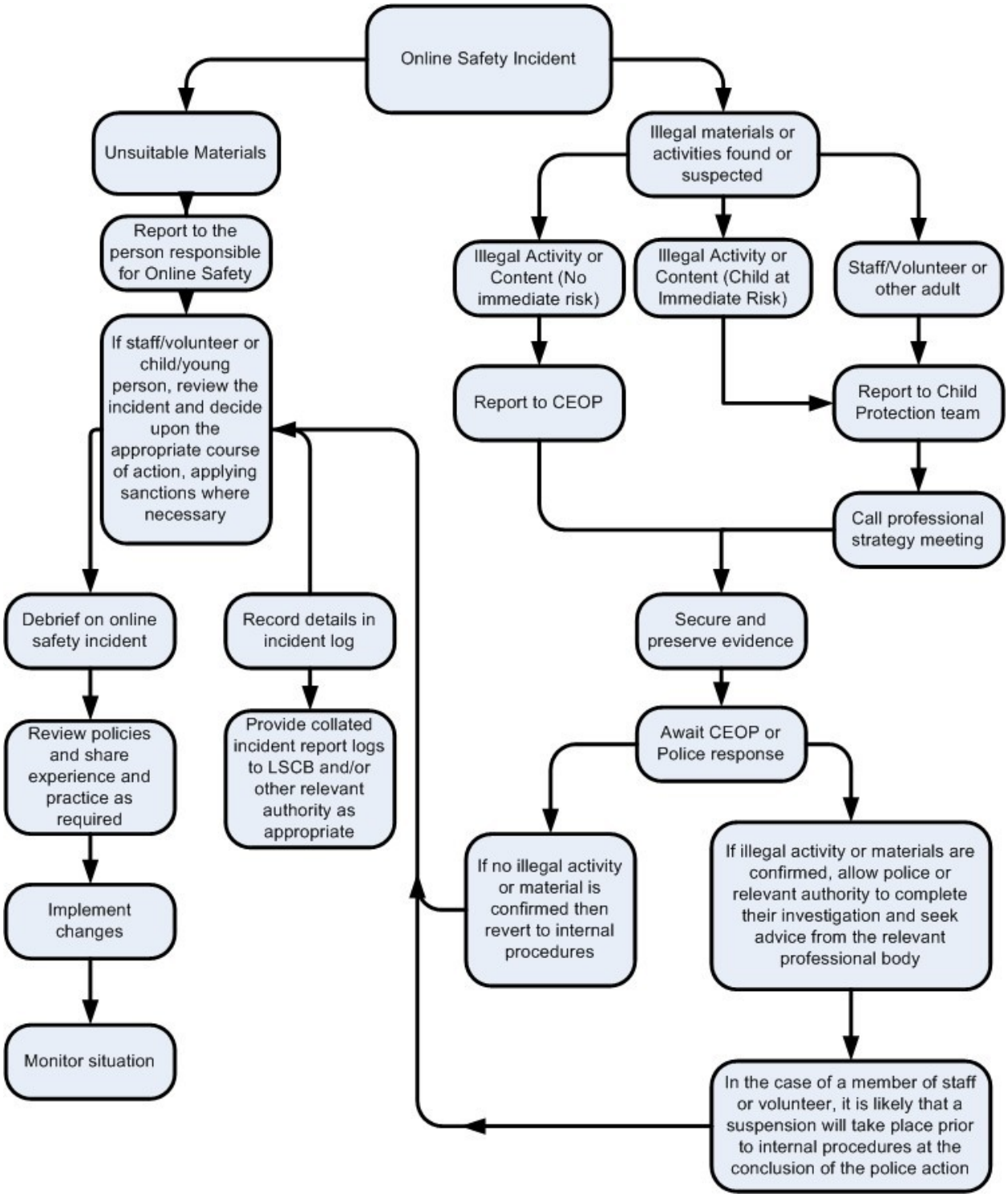
- Just a joke? – lesson plans, activities, a quiz and teaching guide designed to explore problematic online sexual behaviour with 9-12 year olds.

Information Commissioner's Office: GDPR guidance and resources

- Data-sharing information hub – resources to help schools and colleges comply with data protection legislation including UK GDPR.

Appendices

Appendix 1 – Process Flowchart



Appendix 2 – 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	–
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	–
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
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
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	–
Breaching copyright or licensing regulations	Warning	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
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

Scenario	Action 1	Action 2	Action 3	Action 4	Action 5
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, using another person's account	Disciplinary action	removal of network / internet access rights	refer to class teacher / tutor	inform parents / carers	–
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
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	–
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

Appendix 3 – Staff Incidents and Actions

Scenario	Action 1	Action 2	Action 3	Action 4	Action 5
Actions which could compromise the staff member's professional standing	Disciplinary action	suspension	refer to Principal	refer to RHoS / HR	
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	
Accidentally accessing offensive or pornographic material and failing to report the incident	Warning	disciplinary action	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	
Deliberately accessing or trying to access material that could be considered illegal	Suspension	refer to Principal	refer to RHoS / HR	refer to Police	
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	
Breaching copyright or	Warning	disciplinary action	suspension	refer to Principal	refer to RHoS / HR

Scenario	Action 1	Action 2	Action 3	Action 4	Action 5
licensing regulations					
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
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	
Deliberate actions to breach data protection or network security rules	Disciplinary action	suspension	refer to Principal	refer to RHoS / HR	refer to Police
Inappropriate personal use of the internet / social media / personal email	Warning	disciplinary action	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