

## Online Safety Policy 2026

**Approved by:** Rosa Tortosa

**Last reviewed on:** June 2026

**Date:** June 2026

**Next review due by:** June 2028

### Purpose

Online safety is a fundamental component of protection at MAGNO International School. This policy helps protect the school community from risks such as exposure to harmful content, cyberbullying, grooming, and radicalization. It helps ensure that students can access the benefits of the internet safely by minimizing potential risks and harm.

### 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 inside and outside the school.

When the school places students with an alternative provider, it remains responsible for the protection of those students. An assessment will be conducted with the provider in accordance with this policy, and the school must obtain written confirmation that online security controls are in place.

### Legislation and guidance

The legal guide Keeping Children Safe In Education (KCSIE) establishes definitions of online risks, including those related to AI and deepfake technologies. At the local level, this protection is implemented through Law 26/2018 of December 21, of the Generalitat Valenciana, on the rights and guarantees of children and adolescents, complemented by the Valencian Strategy for Children and Adolescents and the campaigns of the regional cybersecurity center CSIRT-CV.

Under the UK Education and Inspections Act 2006, headteachers have reasonable authority to regulate student behavior outside school premises, and staff can impose disciplinary measures for misconduct, including online bullying, related to school membership. The Education Act 2011 (Section 24b) extends these powers to include the search of electronic devices and the deletion of data. Within the framework of the LOMLOE (Organic Law 2011 on the Modification of the Organic Law on Education) and the State School Council agreement, the Valencian Community regulates the use of mobile devices in its Resolution of April 17, 2024, and Decree 193/2025 of December 12, requiring schools to define misuse in their Code of Conduct and internal regulations.

The school will address online misconduct through a series of policies and will inform parents when inappropriate behavior is identified outside of school.

### Types of risks

The range of issues classified within online security is considerable and constantly evolving, but it can be categorized into four risk areas:

**Content:** being exposed to illegal, inappropriate or harmful content, including AI-generated images, audio or video.

*Examples include pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalization, extremism, impersonation, disinformation, misinformation (including fake news), and conspiracy theories.*

**Contact:** being exposed to harmful online interactions with other users.

*Examples include peer pressure, commercial advertising, or adults posing as children or young people with the intention of manipulating or exploiting them for sexual, criminal, financial, or other purposes.*

**Conduct:** online behavior that increases the likelihood of or causes harm or misconduct.

*Examples include creating, sending, receiving, or sharing explicit images (both consensual and non-consensual, of nudity and semi-nudity and/or pornography), online harassment, or bullying.*

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

## Inappropriate content

It is expected that:

Users are effectively and reliably prevented from generating or accessing harmful and inappropriate content; The filtering standards are effectively maintained throughout the duration of a conversation or interaction with a user;

The filtering will be adjusted based on different levels of risk, age, suitability and user needs — for example, users with special educational needs and disabilities (SEND);

Multimodal content is effectively moderated, including the detection and filtering of prohibited content in various languages, images, common spelling errors, and abbreviations.

All content moderation capabilities are maintained regardless of the device used, including Bring Your Own Device (BYOD) and smartphones when accessing products from an educational institution account.

Content is moderated based on an appropriate contextual understanding of the conversation, ensuring that the generated content is context-sensitive.

The filtering is regularly updated in response to new or emerging types of harmful content and AI tools that users can access.

## Roles and responsibilities

All users, including external guests, must read and accept the acceptable use policy before accessing and using school systems and local and online networks. The following online safety responsibilities apply to specific roles:

### School Council

Approval of the Online Security Policy

Review the effectiveness of the policy based on the RHoS comments

### Regional Director of Schools (RHoS)

He serves as a member of the Operational Board responsible for Online Safety, which includes:

Hold regular meetings with the Online Safety Coordinator/Designated Protection Officer/Director;

review and approve any policy changes;

monitor online security incidents and reports;

Report incidents to the Operational Board.

### Executives and senior leaders

Ensuring the safety of the school community

Ensure that a comparable authority or power exists under local legislation

Ensure there is a system in place to monitor, report, and receive incident reports from the Online Security Officer/Designated Security Liaison (DSL)

Delegate daily online security responsibilities to the Online Security Officer / Designated Protection Officer (DSL)

Ensure that all staff receive adequate training

### Online Security Officer/Designated Protection Officer (or Deputy Director)

### Lead the Online Security Group

Manage daily online security incidents and maintain a log of all incidents

Review the process and policy and suggest improvements or identify any non-compliance to the management team

Provide training and advice to all staff

Liaison with technical staff and external authorities

### Network/IT Manager and Technical Staff

Stay up to date on online security policy, practices, and training

To guarantee the physical security of the school's technical infrastructure

Implement and monitor online security measures and ensure they are up to date, including firewall and antivirus protection.

Ensure that all technology related to online access is protected in accordance with local regulations, the Online Security Policy, and group references.

Ensure that any external service provider you hire follows online security measures and is fully informed about school processes before working at the school.

Ensure that any messaging and collaboration platform is monitored for misuse and, in the event of an incident, inform the Online Security Officer and the management team for investigation.

Ensure that physical access to computer systems is restricted to the appropriate level and that users have clearly defined access rights (this includes online and removable storage, data systems for staff and students, organizational data and internet access).

Ensure that all students and staff have a username and password that meet the security standards set out in the Password Policy, and that generic user accounts are not used on any school system.

Ensure that all master administrator usernames and passwords are stored in an encrypted vault, and that the Principal has access to it in case of emergencies to maintain business continuity.

Make sure all software licenses are up to date and cover the number of users/devices in use at the school.

Ensure that all internet access is filtered according to the appropriate age and role level at the school, that firewalls and security gateways are up to date, and that security controls reflect the protection controls established in the Protection Controls Policy.

Supports the Online Security Officer/DSL to ensure that there is a system in place that can monitor, record, and report online security incidents.

Ensure that the IT Acceptable Use Policy is available to staff, students, parents, and external collaborators, and is enforced **before** granting access to school systems and networks.

Conduct an annual cybersecurity risk assessment and review it every quarter.

Develop and implement a plan to back up school data and review it every year

Report all cyberattacks

### Teaching and support staff

Read, understand, and comply with the Online Security and Acceptable Use of IT policies

Stay up to date on online security issues

Integrate online safety into the curriculum

Supervise and guide students' use of digital technologies

Report any misuse to the Online Security Officer and the senior management team for investigation

Ensure that all communications with students and parents are conducted through official school systems, and that conversations are always professional in nature.

Make sure students understand the Internet Security Policy and how to avoid plagiarism and copyright infringement

In classes where internet use is pre-planned, students should be guided to sites that have been proven to be appropriate for their use, ensuring that processes are in place to deal with any inappropriate material found in internet searches.

Monitor and implement current policies regarding devices whenever the use of digital technologies, mobile devices, cameras, etc. is permitted in classrooms and other school activities

### Students

Understand online security 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 the recommendations on best practices, taking photos safely, proper mobile phone use, and develop an understanding of online harassment.

## Parents

Support the school's online safety policies

Monitor your children's online activities

Understand the importance of good online security and what this situation is like, paying special attention to:

Proper use of personal devices

Digital photo and video images at school events and around

Secure access and sharing of guidance on the sections of educational platforms for parents and online student records

## Education and training

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

### Student Education

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

**Curriculum delivery:** A structured online security curriculum will be delivered through Computer Science, PSHE and other relevant subjects, with regular reinforcement.

**School-wide messaging:** Key online safety messages will be integrated into assemblies, tutoring, and pastoral programs.

**Critical thinking:** Students will be taught to critically evaluate online content and verify its accuracy.

**Digital responsibility:** Lessons will include guidance on how to recognize sources and respect copyright.

**Resilience to radicalization:** Students will receive support to develop resilience through safe discussions on controversial topics and an understanding of civic engagement in the face of extremism.

**Acceptable Use:** Students will be trained on the importance of the IT Acceptable Use Policy and encouraged to use technology responsibly both inside and outside of school.

**Staff Role Model:** Staff will model the proper 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 implemented to manage exposure to inappropriate content.

**Supervision:** When students have open access to the internet, 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. These requests must be auditable and justified, and may be approved by the head of department, in consultation with the RHoS when necessary.

### Parental education and involvement

Parents play a vital role in guiding and monitoring their children's online behavior, although 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:

Activities linked to the curriculum

Communications (e.g., letters, newsletters, website, learning platform)

Parent sessions, workshops and events

campaigns (for example, Safer Internet Day)

Guidance to trusted resources (e.g., [saferinternet.org.uk](http://saferinternet.org.uk), [childnet.com](http://childnet.com))

Providing information and resources to support online safety at home

### Education and Participation of Staff/Volunteers

All staff receive formal, audited online security training as part of their ongoing training and a mandatory training plan

New staff receive online security training as part of their induction, which is completed within the first 3 weeks.

All staff review and formally agree to the Online Security Policy and other related policies as part of the year-end activities or onboarding during the year

## Regional Director of Schools (RHoS) and School Board

Participate in regular formal and audited training in Online Security as part of your continuing education and mandatory training plan

## Handling misuse incidents

This section covers the steps necessary to manage incidents and aims to ensure that:

Clear procedures are followed for incident management; and

Serious incidents are reported immediately to the relevant authorities.

### Incidents

When investigating incidents, school officials:

involve at least two senior officials to ensure accountability;

Use a designated computer that is not accessible to students. This device may be required by the police.

ensure that researchers have monitored and recorded internet access;

maintain a timeline of events for possible police reports;

Record URLs and describe concerning content. Capturing and storing screenshots can be beneficial, but you should exclude images of child abuse;

Following the investigation, the center's management will determine if the concern is valid and will take appropriate action.

internal disciplinary measures;

referral to the Regional Director of Schools and/or other relevant authorities;

Police intervention.

### Mandatory Referral to the Police

Certain incidents must be reported to the police without exception:

Images of child abuse

Grooming behavior

sending obscene material to a child

violations of the Obscene Publications Act

Criminally racist content

Promotion of terrorism or extremism

Other criminal activities

### Protection Measures

The computer used for the investigation must be isolated, to preserve evidence and prevent the possibility of manipulation.

All steps taken must be recorded in a chronological log to create a clear trail of evidence for protection and legal purposes.

The completed research form/record should be kept for reference.

### Actions and sanctions

It is important that any incident be resolved as quickly and proportionately as possible. It is also important that members of the school community are informed that incidents have been addressed.

The Appendix includes a process flow diagram and suggested actions and sanctions for incidents.

## Monitoring and review

This policy has been developed by a working group composed of:

- Director / Senior Leaders
- Online Security Officer / Designated Protection Officer
- Staff (teachers, support staff, technical staff)
- Regional Director of Schools / Board
- Parents
- Student Representatives

## Calendar for monitoring, review, and further development

|              |                                                                                                                   |
|--------------|-------------------------------------------------------------------------------------------------------------------|
| Approval V1: | By the Board on 31/07/2025                                                                                        |
| Monitoring:  | By the Senior Leadership Team, at least once a year                                                               |
| Reports:     | Annually to the Regional Director of Schools and the Council,<br>with immediate notification in serious incidents |
| Review:      | Annually, or as needed based on new developments or<br>subsequent incidents, by RHoS on behalf of the Board       |

## Related policies

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

- Protection Policy
- School behavior and anti-bullying policies
- Acceptable use of IT policies, AI, passwords, social media, and security controls
- Keeping Children Safe in Education (KCSIE) 2026

## Useful references

**UK Safer Internet Centre** : [saferinternet.org.uk - guides and resources](https://saferinternet.org.uk/guides-and-resources)

*In particular, the UK's Safer Internet Centre has produced a series of webinars for teachers on behalf of the DfE, to inform and support schools in their filtering and monitoring responsibilities: [Proper Filtering and Monitoring](#)*

**UK Government:** [Education, training and skills - gov.uk](https://www.gov.uk/education-training-skills)

[Filtering and monitoring standards](#)

[Cybersecurity standards for schools and universities](#) developed to help them improve their resilience to cyberattacks

[Prevention of school bullying](#) (including cyberbullying)

[Information sharing for people who provide child protection services](#)

**UK Internet Safety Council:** [UKCIS](https://www.ukcis.org/)

[Sharing nudes and semi-nudes](#): advice for schools and universities on how to respond to incidents of consensual and non-consensual sharing of nudes and semi-nudes.

**Childnet:** [Childnet](https://www.childnet.org.uk/)

[Just a joke?](#) – lesson plans, activities, a quiz and a teaching guide designed to explore problematic online sexual behaviors with children aged 9 to 12.

**Information Commissioner's Office:** [GDPR Guidance and Resources](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/)

[Data Sharing Information Hub](#) – resources to help schools and colleges comply with data protection legislation, including the UK GDPR.

## APPENDICES

## Appendix 1 – Process Flow Diagram

## Appendix 2 – Student Incidents and Actions

| Scenery                                                                                            | Action 1                                              | Action 2                                  | Action 3                               | Action 4                       | Action 5           |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------------|-------------------------------------------|----------------------------------------|--------------------------------|--------------------|
| Unauthorized downloading or uploading of files                                                     | Warning                                               | Removal of network/Internet access rights | Consult the teacher/tutor of the class | Inform the parents/care givers | –                  |
| Continued violations of the above, after prior warnings or sanctions                               | Additional penalties for example, detention/exclusion | Removal of network/Internet access rights | Consult the teacher/tutor of the class | Inform the parents/care givers | –                  |
| <u>Accidentally accessing</u> offensive or pornographic material and not reporting the incident    | Warning                                               | Removal of network/Internet access rights | Consult the teacher/tutor of the class | Inform the parents/care givers | –                  |
| <u>accessing</u> or attempting to access offensive or pornographic material                        | Suspension                                            | Removal of network/Internet access rights | consult the director                   | Inform the parents/care givers | Consult the police |
| Deliberately accessing or attempting to access material that could be considered illegal           | Suspension                                            | Removal of network/Internet access rights | consult the director                   | Inform the parents/care givers | Consult the police |
| Using proxy sites or other means to subvert the school's filtering system                          | Disciplinary action                                   | Removal of network/Internet access rights | Consult the teacher/tutor of the class | Inform the parents/care givers | –                  |
| Actions that could bring discredit to the school or undermine the integrity of the school's spirit | Disciplinary action                                   | Removal of network/Internet access rights | Consult the teacher/tutor of the class | Inform the parents/care givers | –                  |
| Violation of copyright or licensing regulations                                                    | Warning                                               | Removal of network/Internet access rights | Consult the teacher/tutor of the class | Inform the parents/care givers | –                  |
| Corrupt or destroy other users' data                                                               | Disciplinary action                                   | Removal of network/Internet access rights | consult the director                   | Inform the parents/care givers | Consult the police |
| Careless use of                                                                                    | Warning                                               | Removal of                                | Consult the                            | Inform the                     | –                  |

|                                                                                                                                                                               |                     |                                           |                                        |                                |                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|-------------------------------------------|----------------------------------------|--------------------------------|--------------------|
| personal data, for example, storing or transferring data in an unsecured manner                                                                                               |                     | network/Internet access rights            | teacher/tutor of the class             | parents/care givers            |                    |
| Allowing others to access the school network by sharing usernames and passwords or attempting to access or actually accessing the school network using someone else's account | Disciplinary action | Removal of network/Internet access rights | Consult the teacher/tutor of the class | Inform the parents/care givers | –                  |
| Deliberate actions to violate data protection or network security regulations                                                                                                 | Disciplinary action | Removal of network/Internet access rights | consult the director                   | Inform the parents/care givers | Consult the police |
| Inappropriate personal use of the internet / social media / personal email                                                                                                    | Warning             | Removal of network/Internet access rights | Consult the teacher/tutor of the class | Inform the parents/care givers | –                  |
| Sending an email, text message, or message that is considered offensive, harassing, or of a stalking nature                                                                   | Disciplinary action | Removal of network/Internet access rights | consult the director                   | Inform the parents/care givers | Consult the police |

## Appendix 3 – Staff Incidents and Actions

| Scenery                                                                                            | Action 1            | Action 2             | Action 3             | Action 4             | Action 5           |
|----------------------------------------------------------------------------------------------------|---------------------|----------------------|----------------------|----------------------|--------------------|
| Actions that could compromise the professional standing of the staff member                        | Disciplinary action | Suspension           | consult the director | consult RHoS / HR    |                    |
| Unauthorized downloading or uploading of files                                                     | Warning             | Disciplinary action  | Suspension           | consult the director | consult RHoS / HR  |
| Continued violations of the above, after prior warnings or sanctions                               | Disciplinary action | Suspension           | consult the director | consult RHoS / HR    |                    |
| <u>Accidentally</u> accessing offensive or pornographic material and not reporting the incident    | Warning             | Disciplinary action  | consult the director | consult RHoS / HR    |                    |
| <u>accessing</u> or attempting to access offensive or pornographic material                        | Suspension          | consult the director | consult RHoS / HR    | Consult the police   |                    |
| Deliberately accessing or attempting to access material that could be considered illegal           | Suspension          | consult the director | consult RHoS / HR    | Consult the police   |                    |
| Using proxy sites or other means to subvert the school's filtering system                          | Disciplinary action | Suspension           | consult the director | consult RHoS / HR    |                    |
| Actions that could bring discredit to the school or undermine the integrity of the school's spirit | Disciplinary action | Suspension           | consult the director | consult RHoS / HR    |                    |
| Violation of copyright or licensing regulations                                                    | Warning             | Disciplinary action  | Suspension           | consult the director | consult RHoS / HR  |
| Corrupting or destroying other users' data or deliberately damaging hardware or software           | Disciplinary action | Suspension           | consult the director | consult RHoS / HR    | Consult the police |
| Careless use of personal data, for example, storing or transferring data in an unsecured manner    | Warning             | Disciplinary action  | consult the director | consult RHoS / HR    |                    |
| Allowing others to access the school                                                               | Disciplinary action | Suspension           | consult the director | consult RHoS / HR    |                    |

|                                                                                                                                      |                     |                     |                      |                   |                    |
|--------------------------------------------------------------------------------------------------------------------------------------|---------------------|---------------------|----------------------|-------------------|--------------------|
| network by sharing usernames and passwords or attempting to access or gain access to the school network using someone else's account |                     |                     |                      |                   |                    |
| Deliberate actions to violate data protection or network security regulations                                                        | Disciplinary action | Suspension          | consult the director | consult RHoS / HR | Consult the police |
| Inappropriate personal use of the internet / social media / personal email                                                           | Warning             | Disciplinary action | consult the director | consult RHoS / HR |                    |
| Use of personal email / social media / instant messaging / text messaging to conduct digital communications with students            | Disciplinary action | Suspension          | consult the director | consult RHoS / HR |                    |
| Sending an email, text message, or message that is considered offensive, harassing, or of a stalking nature                          | Disciplinary action | Suspension          | consult the director | consult RHoS / HR | Consult the police |