

ANGLO EUROPEAN SCHOOL



Online Safety Policy

Last reviewed 06.10.2026

This policy is regularly reviewed following recommended guidelines

Online Safety Policy Statement:

Our school is committed to safeguarding and promoting the welfare of children and young people in accordance with statutory guidance, including Keeping Children Safe in Education (KCSIE), Working Together to Safeguard Children, and the Prevent Duty. Online safety is an integral part of the school's safeguarding framework. The school recognises that technology, including artificial intelligence (AI), is embedded in children's lives and presents both educational opportunities and safeguarding risks.

This policy applies to all students, staff, governors, visitors, and any person working on behalf of the school.

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support groups of students that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Ensure that students develop the knowledge and skills to use digital technologies safely and responsibly.
- Ensure staff understand their safeguarding responsibilities in relation to online activity and AI use.
- Ensure that we provide appropriate filtering, monitoring, and oversight systems
- Assess the risks associated with emerging technologies, including AI, and identify and manage them effectively

The 5 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as 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 – personal online behaviour that increases the likelihood of, or causes, harm, such as 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

AI – the school recognises risks associated with Artificial Intelligence tools, including but not limited to:

- Generation of inappropriate, misleading, or harmful content
- AI-enabled grooming or manipulation via chatbots or generated personas
- Deepfake images, audio, or video used to deceive or harass
- Over-reliance on AI tools leading to academic misconduct (plagiarism)
- AI tools collecting or processing personal data without consent
- Bias or inaccurate outputs affecting learning or decision-making

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, **Keeping Children Safe in Education** and supporting non-statutory guidance including:

- Teaching online safety in schools
- Preventing and tackling bullying (DfE guidance) and advice on cyberbullying for headteachers and school staff
- Relationships Education, Relationships and Sex Education and Health Education
- Searching, Screening and Confiscation

It also refers to the DfE's guidance on protecting children from radicalisation, in line with the Prevent Duty

It reflects legislation including (but not limited to):

- Education Act 1996
- Education and Inspections Act 2006
- Equality Act 2010
- Education Act 2011 (including powers relating to searching and confiscation)

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

Roles and responsibilities:

The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Governing Body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Governing Body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Governing Body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher and Governing Body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with IT managers to make sure the appropriate systems and processes are in place
- Working with the Headteacher, Assistant Headteacher (Data, Data, Examinations & Careers) and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or Governing Body
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

Assistant Headteacher Data, Examinations & Careers

The Assistant Headteacher with oversight for Data, Examinations & Careers is responsible for:

- Liaising with the school's IT provider, namely Sweethaven.
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensuring that conduct a full security check and monitoring the school's IT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing.
- Following the correct procedures by alerting the DSL if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents and Carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (appendices 1 and 2)
- Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
 - What are the issues? – [UK Safer Internet Centre](#)
 - Hot topics – [Childnet International](#)
 - Parent resource sheet – [Childnet International](#)
 - [National Online Safety](#)

Visitors

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

Filtering and Monitoring

The school uses Smoothwall filtering and monitoring services to support the safeguarding of students and staff. Smoothwall provides web filtering, digital monitoring and safeguarding alerts designed to identify potentially harmful, inappropriate or illegal online activity. Safeguarding concerns identified through these systems are reviewed by the Designated Safeguarding Lead and Deputies and managed in accordance with the Child Protection Policy. The effectiveness of filtering and monitoring systems will be formally reviewed at least once every academic year by SLT, with support from the DSL and DDSs and IT support provider. A written record of the review, including testing outcomes, identified risks and planned actions, will be retained.

Educating students about online safety

Students will be taught about online safety as part of the Anglo European School Curriculum.

In Key Stage 3, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

In Key Stage 4, students will be taught:

- To understand how changes in technology affect safety, including new and emerging technologies such as artificial intelligence (AI), and how to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of exposure to harmful, inappropriate or illegal online content, including content that promotes self-harm, violence, or extremism
- That sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviour, can damage self-image and relationships, and may negatively influence behaviour
- That sharing and viewing sexual images of children (including youth-produced sexual imagery) is a criminal offence and can carry severe penalties, including imprisonment
- How information and data is generated, collected, shared and used online

- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report or access support
- How people communicate, recognise and respect consent, including sexual consent, and how consent can be freely given, withdrawn, or misunderstood, including in online contexts
- How to critically evaluate online information and recognise misinformation, disinformation and AI-generated or manipulated content
- What to do if they encounter unsafe or illegal online material and where to access support

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND

Educating parents about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website This policy will also be shared with parents/carers.

Online safety will also be covered during parental information evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

Online bullying:

Definition

This is bullying which takes place online, such as through social media, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing online bullying

The use of mobile phones is not permitted in our school. We have taken this decision in order to keep students safe and minimise the chances of online bullying, To help prevent online bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that

students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss online bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover online bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on online bullying, its impact and ways to support students, as part of safeguarding training.

The school provides information on online bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of online bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Online Sexual Harassment

Students will be explicitly taught about online sexual harassment, the influence of pornography, misogynistic online content, AI-generated imagery and strategies for seeking support when encountering harmful content online.

Mobile Phones and Electronic Devices

Students in Years 7 to 11 may bring mobile phones and other electronic devices to school; however, these devices must remain secured and inaccessible throughout the school day in accordance with the school's mobile phone procedures. Students are not permitted to use mobile phones or other personal electronic devices during lessons, tutor time, break or lunchtime, clubs, educational activities, or at any other time during the school day unless expressly authorised by a member of staff for a specific educational purpose.

Sixth Form students may use mobile phones in designated Sixth Form areas and within lessons where permission has been granted by the teacher. Sixth Form students must not use mobile phones, headphones or other personal electronic devices whilst moving around the school site. Any misuse of a mobile phone or electronic device will be dealt with in accordance with the school's Behaviour Policy and may result in confiscation of the device.

The Headteacher, or a member of staff authorised by the Headteacher, may search for and confiscate an electronic device, including a mobile phone, where there are reasonable grounds to suspect that the device:

- Poses a risk to the safety or wellbeing of students or staff;
- Is a prohibited item under the school's rules;
- Contains evidence relating to a breach of school rules or a criminal offence; or
- Has been used in a manner that may place a child at risk of harm.

Before carrying out a search, the authorised member of staff will, where appropriate:

- Assess the urgency of the situation and any immediate safeguarding risks;
- Seek advice from the Headteacher or Designated Safeguarding Lead (DSL) if the matter is not urgent;
- Explain the reason for the search and the process to the student; and
- Seek the student's cooperation.

Authorised staff may examine the contents of a confiscated device where they have a lawful and reasonable basis to do so. A device may be examined where there is reason to believe that it has been used to:

- Cause harm to an individual;
- Undermine the safe and orderly running of the school;
- Facilitate bullying, harassment or abuse, including online abuse;
- Commit, or assist in committing, a criminal offence; or
- Place a child at risk of significant harm.

Where inappropriate content is discovered, the member of staff will immediately liaise with the DSL to determine the appropriate safeguarding, disciplinary or legal response. If any content is believed to place a person at risk of harm, safeguarding considerations will take precedence.

In exceptional circumstances, data or files may be deleted from a device where there is a good reason to do so and where the material does not constitute potential evidence of a criminal offence. Where material may constitute evidence, it will be preserved and the device passed to the police as soon as reasonably practicable. Staff may request that a student or parent/carer delete material where appropriate. If they refuse and the material is likely to cause harm, authorised staff may arrange for its deletion in accordance with statutory guidance.

If a member of staff suspects that a device contains an indecent image of a child, including a nude or semi-nude image, they will:

- Not view, copy, print, share or delete the image;
- Confiscate the device and secure it appropriately;
- Report the matter immediately to the DSL; and
- Follow the procedures set out in the school's Child Protection and Safeguarding Policy and the latest Department for Education and UKCIS guidance.

All searches of students and their devices will be carried out in accordance with the Department for Education's *Searching, Screening and Confiscation* guidance, the UKCIS guidance *Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People*, and the school's Behaviour and Safeguarding Policies. Any complaints relating to the searching of, examination of, or deletion of material from electronic devices will be managed through the school's Complaints Procedure.

Artificial Intelligence (AI)

The school recognises that artificial intelligence (AI) technologies are becoming increasingly integrated into everyday life and education. AI tools offer significant opportunities to support teaching, learning and productivity; however, they also present emerging safeguarding, privacy and ethical risks.

The school acknowledges that AI-generated content may be used to create false, misleading, manipulated or sexualised images, audio recordings or videos of students, staff or members of the wider community. This includes the creation and sharing of so-called "deepfakes". Such behaviour has the potential to cause significant harm and will be treated as a safeguarding concern. Any incidents will be investigated and managed in accordance with the school's Child Protection and Safeguarding Policy, Behaviour Policy and relevant statutory guidance.

Staff, students and parents/carers may be familiar with generative AI tools such as ChatGPT, Microsoft Copilot and Google Gemini. While these technologies can enhance learning and creativity, users should be aware that AI-generated content may be inaccurate, biased, misleading or inappropriate. Students will therefore be taught how to use AI responsibly, critically evaluate AI-generated content, recognise manipulated media and identify potential misinformation or disinformation.

The school will not tolerate the use of AI to bully, harass, intimidate, exploit or harm others. Any misuse of AI, including the creation or sharing of harmful, abusive or inappropriate content, will be addressed in line with the school's behaviour and safeguarding procedures.

Staff should exercise professional judgement when using AI tools and ensure that any use complies with data protection, confidentiality, copyright and safeguarding requirements. Before introducing new AI applications or platforms, appropriate risk assessments should be undertaken to ensure that they are safe, lawful and suitable for educational use.

Staff using work devices outside of school

All teaching staff and some support staff have school devices which can be used outside the workplace. These staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's online safety policy. Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from our IT provider.

Cyber Security

- We place a high importance on cyber security, acknowledging cyber security as a safeguarding issue because compromise of systems can expose children to risk. Staff have received training, advice and guidance on:
 - using MFA where possible
 - phishing awareness
 - secure handling of personal data
 - incident reporting
 - ransomware response arrangements
 - cooperation with Smoothwall

Responding to misuse of IT facilities

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour and online safety policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including online bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
- Abusive, harassing and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

Develop better awareness to assist in spotting the signs and symptoms of online abuse

Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks

Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL [and deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the Governing Body and the policy will consider and reflect the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Safeguarding record retention

Records relating to online safety incidents will be retained in accordance with safeguarding record-keeping procedures and data protection requirements.

Routes to reporting

Students may report online safety concerns to any member of staff, the DSL team, anonymously through the school's reporting systems, or through external reporting services where appropriate.