

E-SAFETY/ONLINE SAFETY POLICY

September 2026

1. AIMS

EIFA International School ("EIFA", "School", "we", "us" or "our") aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, and volunteers
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole School community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Address the four main categories of online risk defined by the DfE: **Content** (exposure to harmful/inappropriate material), **Contact** (interaction with unsafe adults or peers, including dynamic AI interfaces), **Conduct** (personal online behaviour, harassment, and cyberbullying), and **Commerce** (financial scams, online gambling, and unauthorised purchases).

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyberbullying: advice for headteachers and school staff](#)
- [Searching, screening and confiscation](#)
- [Relationship and Sex Education Guidance](#)

It also refers to the Department's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyberbullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. ROLES AND RESPONSIBILITIES

3.1 The Board of Directors

The Board of Directors has overall responsibility for monitoring this policy and holding the Head of School to account for its implementation.

The Board of Directors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the School's ICT systems and the internet
- Ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks
- Review the effectiveness of the School's filtering and monitoring systems

- 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 the standards, if required
- Ensure that Online Safety is a running and interrelated theme while devising and implementing the School's approach to safeguarding
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for pupils with special educational needs and/or disabilities (SEND).
- Ensure it has a member with specific oversight of filtering and monitoring effectiveness and DfE compliance
- Ensure that minutes of Board meetings formally record the annual review of filtering and monitoring systems and DfE standards discussions.

3.2 The Head of School

The Head of School is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the School.

3.3 The Designated Safeguarding Lead(s) (DSL or DSLs)

Details of the School's Designated Safeguarding Leads are set out in our Child Protection and Safeguarding Policy.

The DSLs take lead responsibility for online safety in School, in particular:

- Supporting the Head of School in ensuring that staff understand this policy and that it is being implemented consistently throughout the School
- Working with the Head of School and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the School's Behaviour Management Policy
- Updating and delivering staff training on online safety, liaising with other agencies and/or external services if necessary
- Providing reports on online safety in School
- Providing regular reports on online safety in School to the Board of Directors
- 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
- Maintain lead responsibility for understanding the school's filtering and monitoring systems, managing technical escalation alerts, and ensuring these responsibilities are formally detailed in the DSL job description.
- Correlate automated filtering/monitoring alerts (e.g., searches related to self-harm, radicalisation, or harassment) directly with CPOMS records to ensure contextual safeguarding follow-up.

This list is not intended to be exhaustive.

3.4 The School's Senior Leadership

The Senior Leadership are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at School, including terrorist and extremist material
- Ensuring that the School's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check of, and monitoring the School's ICT systems

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on the Child Protection Online Management System (CPOMS) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the School's Behaviour Management Policy
- Ensure that filtering systems completely block access to illegal content specified by the Internet Watch Foundation (IWF) and Counter Terrorism Internet Referral Unit (CTIRU), and verify these protections cannot be bypassed on any account.
- Ensure that school-managed filtering and monitoring protections apply to all school-issued devices both on-site and when used off-site.
- Work with IT providers to assess filtering capabilities regarding encrypted traffic (HTTPS), dynamic AI tool outputs, and embedded applications.

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

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

- Maintaining an understanding this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the School's ICT systems and the internet and ensuring that pupils follow the School's terms on acceptable use
- Working with the DSLs to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the School's 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.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Head of School of any concerns or queries regarding this policy
- Ensure their child has understood and agreed to the terms on acceptable use of the School's ICT systems and internet

Parents 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 fact sheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the School's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils will be taught about online safety as part of the curriculum:

Since September 2020 it has been compulsory for all schools to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stages 2 and 3, will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of Primary School, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In Years 7, 8 and 9 pupils 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

The safe use of social media and the internet will also be covered in other subjects where relevant.

The School will raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. EDUCATING PARENTS ABOUT ONLINE SAFETY

The School will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environments.

Online safety will also be covered during parents' evenings, by specialist speakers.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School, and/or one of the DSLs.

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

6. CYBERBULLYING

6.1 Definition

Cyberbullying takes place online, such as through social networking sites, 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 Management Policy.)

6.2 Preventing and addressing cyberbullying

To help prevent cyberbullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils 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 cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyberbullying with their tutor groups, and the issue will be addressed in assemblies. Consequences for cyberbullying are the same as any other form of bullying, these can be found in our Behaviour Management Policy.

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

All staff and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyberbullying, the School will follow the processes set out in the School's Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the School will use all reasonable endeavours to ensure the incident is contained.

The DSLs will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The Head of School, and any member of staff authorised to do so, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting poses a risk to staff or pupils, and/or:

- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Head of School or DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Head of School or Senior Leadership Team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS' (UK Council for Internet Safety) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Behaviour Policy / searches and confiscation guidance

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents may be familiar with generative chatbots such as ChatGPT and Google Gemini.

EIFA School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deep fakes', where AI is used to create images, audio or video hoaxes that look real. This includes deep fake pornography: pornographic content created using AI to include someone's likeness.

The School will treat any use of AI to bully pupils in line with our Anti-bullying Policy and Behaviour Management Policy

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the School.

Staff and pupils must not input personal, sensitive, or confidential data (including pupil records, assessment data, or identifying details) into unapproved public generative AI tools. Any deployment of AI tools for administrative or educational purposes must comply with the School's Data Protection Policy.

7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils, parents, staff, volunteers and members of the Board of Directors are expected to sign an agreement regarding the acceptable use of the School's ICT systems and the internet. Visitors will be expected to read and agree to the School's terms on acceptable use, if relevant.

Use of the School's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers and visitors (where relevant) to ensure they comply with the above.

8. PUPILS USING MOBILE DEVICES IN SCHOOL

Pupils from Year 7 upwards who bring a mobile device to School must surrender it to the reception storage facility immediately upon arrival. Devices remain locked in this secure storage facility for the duration of the school day and may only be collected at the end of the day.

Mobile devices are **strictly prohibited from being in a pupil's possession or used throughout the entire school day**, including:

- Lessons and tutor time
- Morning break and lunchtimes
- Before and after-school clubs, sports, or extra-curricular activities on school grounds

Any unauthorised possession or use of a mobile device on school grounds will result in immediate confiscation by staff and disciplinary follow-up in line with the Behaviour Management Policy. Any permitted use of mobile devices (for example, during off-site trips) must comply fully with the ICT and Internet Acceptable Use Policy.

Any breach of the Acceptable Use Agreement by a pupil may trigger disciplinary action in line with the School Behaviour Management Policy, which may result in the confiscation of their device.

9. STAFF USING WORK DEVICES OUTSIDE SCHOOL

Staff members using a work device outside School must not install any unauthorised software on the device and must not use the device in any way which would violate the School's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside School. Any USB devices containing data relating to the School must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from IT Services. Work devices must be used solely for work activities.

Staff are not permitted to use their personal devices in School, unless for authentication purposes, or not in the presence of pupils. For more detailed information, staff should refer to the Employee Handbook and Code of Conduct.

10. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the School's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. 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 system or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Disciplinary Procedures and 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 which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. TRAINING

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, threatening, 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 pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSLs 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.

The Member of the Board in charge of Safeguarding 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.

12. MONITORING ARRANGEMENTS

The DSLs log all online safety issues on CPOMS. The School conducts a formally documented annual review of filtering and monitoring effectiveness alongside IT providers and the Board of Directors.

IT staff perform and log regular physical and technical checks across all school networks, guest Wi-Fi networks, and school-issued devices to verify that filtering and monitoring mechanisms remain fully operational.

13. LINKS WITH OTHER POLICIES

This online safety policy is linked to our: Child Protection and Safeguarding Policy, Behaviour Management Policy, Anti-Bullying Policy, Staff Disciplinary Procedures- Misconduct, Data Protection Policy and Privacy Notices, Parent Complaints Procedure and our ICT and Internet Acceptable Use Policy