International School of London

Online Safety Policy
2026-2027

Date reviewed:
September 2026

To be reviewed:
September 2027

Mission statement

Since 1972, we have established a welcoming and inclusive community. Our diverse cultures and languages drive all our learning experiences.

We nurture creativity and curiosity to stimulate deep thinking. We foster insight, compassion and resilience to enable us to play a meaningful part in a changing world.

Vision statement

We celebrate our stories, our worth and our purpose to make a difference in a shared world.

At the International School of London, we believe in:

- Empowering students to maximise their learning opportunities and to fulfil their potential.
- Actively integrating cultural diversity in the curriculum.
- Creating inclusive, vibrant and innovative learning communities.
- Offering a diverse and extensive international programme that supports personal, social and professional growth.

This policy should be read in conjunction with Keeping Children Safe in Education 2026, the Online Safety Act 2023, Working Together to Safeguard Children 2023, the Data (Use and Access) Act 2025, the UK Council for Internet Safety guidance and the Department for Education Filtering and Monitoring Standards. The school recognises that safeguarding responsibilities extend to emerging technologies, including artificial intelligence (AI), generative AI systems and AI-generated content.

The purpose of this policy statement:

The International School of London works with children and families as part of its activities, to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.
-

The policy statement applies to all staff, volunteers, children and young people and anyone involved in any International School of London activities.

Contents

1. Aims 3
2. Legislation and guidance 4
3. Roles and responsibilities 5
4. Educating and curriculum 8
5. Educating parents/carers about online safety 10
6. Cyber-bullying 10
7. Acceptable use of the internet in school 13
8. Pupils using mobile devices in school 14
9. Staff using work devices outside school 16
10. How the school will respond to issues of misuse 16
11. Training 17
12. Monitoring arrangements 18
13. Links with other policies 18
Appendix 1: online safety incident report log 19

---

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils 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 (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 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

Emerging risks

The school recognises the increasing safeguarding risks associated with artificial intelligence (AI) technologies. These may include:

- AI-generated misinformation and disinformation
- Deepfake images, videos and audio
- AI-generated sexualised or abusive images
- AI-enabled bullying and harassment
- Grooming using AI-generated content
- Unsafe advice provided through AI chatbots
- Sharing personal information with AI tools
- Over-reliance on AI without appropriate critical evaluation

These risks will be addressed through curriculum education, staff training, filtering and monitoring arrangements and safeguarding procedures.

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE'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 cyber-

bullying 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 governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

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

The governing board will ensure that an annual documented review of filtering and monitoring systems is undertaken at least once every academic year. The review will be led by the designated member of the Senior Leadership Team responsible for filtering and monitoring, supported by the DSL and ICT staff. Evidence of the review and resulting actions will be retained, 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.

The review will include testing filtering arrangements across all internet-connected devices and all locations used by pupils and staff. Records of these checks will be maintained

The chair of board who oversees online safety is Amin Makarem.

All board members will:

- Ensure 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 (appendix 3)

- 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 pupils 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

3.2 The Head of School and Principals

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

3.3 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 board 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 the ICT team to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT team 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 (see appendix 5) 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 (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- 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.

3.4 Filtering and monitoring lead

The school will identify a member of the Senior Leadership Team with strategic responsibility for filtering and monitoring. This person will work closely with the Designated Safeguarding Lead and ICT Team to review effectiveness, manage identified risks and ensure statutory requirements are met.

3.5 The ICT Team

The ICT team is responsible for:

- 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 pupils 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 ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly 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 (see appendix 5) 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.

3.6 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
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

- 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 by logging it to CPOMs.
- Following the correct procedures by logging it to CPOMs 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 (see appendix 5) 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.

3.7 Parents/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 ICT 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

3.8 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 (appendix 3).

4. Education and curriculum

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

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

By the **end of Primary Years Programme**, 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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

By the **end of Middle Years Programme**, pupils 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 viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- 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 find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant. Students will be taught the risks associated with sharing personal information with AI tools and online platforms.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Students should not upload personal data, images, videos, recordings or confidential school information into publicly available AI systems unless authorised by staff and approved under school procedures.

ISL recognises that pupils with SEND may be at increased risk of online exploitation, manipulation, bullying or misunderstanding online interactions. Online safety education will therefore be differentiated as required to ensure accessibility and effectiveness.

4.1 Mobile Phones and Personal Devices

ISL recognises that online safety and mobile phone use are closely linked. To support students' wellbeing, concentration, safeguarding and responsible use of technology, the school operates a mobile phone-free environment during the school day.

Students in all year groups are expected to switch off mobile phones and store them securely in their lockers upon arrival. Mobile phones, smart watches, headphones and other personal electronic devices must not be used during lessons, tutor periods, break times, lunch times, educational activities or extra-curricular activities unless specifically authorised by the Head of School or required as a reasonable adjustment.

Where students require access to technology for learning, school-managed devices and networks will be used. This enables appropriate filtering, monitoring and safeguarding arrangements to be maintained.

Any breach of these expectations will be managed in accordance with the Mobile Phone Policy, Behaviour Policy and safeguarding procedures.

5. Educating parents/carers 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 parents' 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.

6. Cyber-bullying

6.1 Definition

Cyber-bullying 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

The school recognises that cyberbullying, harassment, image sharing, AI-generated abuse, inappropriate messaging and online exploitation frequently occur through personal mobile devices.

Restricting student access to mobile phones during the school day forms part of the school's safeguarding arrangements designed to reduce opportunities for online harm while students are on site.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, 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 cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-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 cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-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 cyber-bullying, the school will follow the processes set out in the school 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 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.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher 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 headteacher / DSL / appropriate staff member
- 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 DSL / Principal 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

Where there is reasonable cause to suspect that a device contains evidence relating to a safeguarding concern, bullying incident, criminal offence or breach of school policy, authorised staff may search, screen or confiscate a device in accordance with the school's Behaviour Policy, Child Protection Policy and current Department for Education guidance.

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 guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices, sharing nudes, semi-nudes, digitally manipulated images and AI-generated intimate images (including "deepfake" imagery) will be dealt with through the school complaints procedure.

Covert Recording

Students, staff, visitors and parents must not make covert recordings of members of the school community.

Unauthorised audio or video recording may constitute:

- a safeguarding concern
- a disciplinary matter
- cyberbullying
- harassment
- a potential data protection breach

Particular care must be taken in counselling rooms, medical areas, safeguarding meetings, SEND provision, student support areas and any location where confidential information may be discussed.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). 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, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

Recording and Personal Data

Photographs, audio recordings, video recordings and other identifiable information relating to members of the school community may constitute personal data.

Such data must only be collected, processed, stored or shared in accordance with UK GDPR, the Data (Use and Access) Act 2025 and the school's Data Protection Policy.

Personal recording devices must not be used to capture school-related information without authorisation.

8. Pupils using mobile devices in school

The use of mobile devices is set out in our Mobile Phones policy (https://www.isllondon.org/policies).

References to mobile phones and personal electronic devices within this policy include AI-enabled wearables, smart glasses, smart watches, connected audio devices and any technology capable of recording, transmitting or accessing online content.

ISL operates a mobile phone-free environment during the school day in line with the school's Mobile Phone Policy. Parents should not contact students directly via mobile phone during the school day.

Any urgent messages should be communicated through the School Front Office. Students wishing to contact parents during the school day should do so through authorised school procedures and with staff support.

Students may bring mobile phones to school for safety and travel purposes; however, mobile phones, smart watches, headphones and personal electronic devices must not be used during the school day except where specifically authorised by the Head of School or where a reasonable adjustment is required.

Online safety, safeguarding and appropriate technology use are supported through clear restrictions on personal device use and through supervised access to school technology systems. Students are not permitted to use mobile phones, smart watches, headphones or other personal electronic devices during the school day. The school day begins when students arrive on site and ends when students leave the school premises. Mobile phones will not be permitted to be used at any after school extra-curricular clubs.

Mobile phones must be switched off and stored in student lockers unless otherwise authorised by the Head of School.

On arrival, mobile phones should be switched off and placed in students' lockers. It should not be seen or heard (including vibrate) throughout the school day.

The phone can be switched back on upon leaving the school site. Not before and not during any period of social time (break or lunch)

Any student found using or known to have used their phone during the school day will have their phone confiscated and returned at 3:30pm via the pastoral team. Parents will be informed.

ISL supports the Department for Education expectation that schools should operate as mobile phone-free environments during the school day except where specific educational, accessibility or safeguarding reasons exist.

College

College students are expected to use school-provided devices for learning. Mobile phones may not be used during lessons, meetings, Directed Study Hours or Supervised Study Hours in line with the Mobile Phone Policy.

Any additional access arrangements will be determined by school leadership. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

AI Wearable Technology

The school recognises that advances in artificial intelligence and wearable technology present new opportunities as well as safeguarding, privacy and data protection risks.

AI-enabled wearable devices may be capable of recording, transmitting, analysing or storing audio, video, images, location data or personal information without the knowledge of others. Such devices may also enable real-time communication, internet access, facial recognition, image analysis or the generation of AI-created content.

For the purposes of this policy, AI wearables include, but are not limited to:

- Smart glasses and AI-enabled glasses
- Smart watches with communication or recording capabilities
- Wearable cameras
- Smart earbuds and headphones with AI assistants
- Smart rings and other connected wearable devices
- Any wearable technology capable of recording, processing or transmitting information

To safeguard students, staff and visitors, students must not use AI-enabled wearable devices during the school day unless specifically authorised by the Head of School or required as a reasonable adjustment under the Equality Act 2010.

The unauthorised use of AI wearables to record, photograph, livestream, monitor, communicate with others, access online content or collect personal information is prohibited and may result in disciplinary action.

Particular care must be taken to protect confidential and sensitive information. Recording or capturing images, audio or video in classrooms, counselling areas, medical rooms, safeguarding meetings, examinations, changing facilities or other private spaces is strictly prohibited unless expressly authorised.

Students will be educated about the responsible, ethical and safe use of emerging technologies, including artificial intelligence, deepfake technologies and AI-enabled wearable devices. The school will review emerging risks regularly and update safeguarding procedures as technology develops.

Any misuse of AI-enabled wearable technology that raises safeguarding concerns, invades privacy, facilitates bullying, harassment, impersonation, the creation or sharing of manipulated content, or breaches data protection requirements will be managed in accordance with the school's Safeguarding and Child Protection Policy, Behaviour Policy, Data Protection Policy and Mobile Phone Policy.

9. Staff using work devices outside school

All 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 terms of acceptable use, as set out in appendix 3.

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 IT Team or DSL.

Staff should not use personal mobile phones in the presence of students except where specifically authorised or in an emergency.

Staff should communicate with students and parents using approved school communication systems such as Microsoft Teams and school email.

Personal mobile phones must never be used to photograph, record or communicate with students. School-issued devices and approved school systems must be used instead.

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 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.

Cyber Security

The school recognises cyber security as an important safeguarding responsibility.

Appropriate technical and organisational measures will be implemented to protect personal data and school systems from unauthorised access, malware, phishing attacks, ransomware and data breaches.

Any cyber security incident that may impact the welfare or safety of children will be treated as a safeguarding concern and reported in accordance with safeguarding procedures

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-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 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 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.

Annual safeguarding and online safety training will include:

- AI-enabled risks and harms
- Deepfake and manipulated content
- Emerging online trends
- Filtering and monitoring responsibilities
- Cyber security awareness
- Online misogyny, harassment and harmful online culture

Staff will understand that emerging technologies may present new safeguarding risks and should report concerns promptly through safeguarding procedures.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Online Safety Coordinator. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

The DSL will complete and formally review an Online Safety Risk Assessment annually. This assessment will consider emerging technologies, AI developments, pupil vulnerabilities, filtering effectiveness, local safeguarding trends and lessons learned from safeguarding incidents.

13. Links with other policies

This online safety policy is linked to our:

- Mobile Phone Policy
- Child Protection and Safeguarding Policy
- Acceptable Use Agreement
- Behaviour Policy
- Anti-Bullying Policy
- ICT Acceptable Use Policy
- Data Protection Policy
- Staff Code of Conduct

Appendix 1: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

At ISL London, Safeguarding and promoting the welfare of children is everyone's responsibility. Everyone who comes into contact with children and their families has a role to play. In order to fulfil this responsibility effectively, all practitioners should make sure their approach is child-centred. This means that they should consider, at all times, what is in the best interests of the child.

Contact details

Online safety co-ordinator

Name: Raul Rodriguez
Phone/email: 0208 9925823; rrodriguez@isllondon.org