CITY OF LONDON SCHOOL FOR GIRLS

ONLINE DIGITAL AND ESAFETY POLICY

Policy reviewed by:	Michael Martyn, Susannah Gilham, Rachel Brincat, Adam Zivanic, Andrew Lindsey
Date policy last reviewed:	September 2023
Policy approved by:	Board of Governors
Date of approval:	22nd September 2023
Next review due:	September 2024

This policy should be read in conjunction with:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Pupil Acceptable Use Policies (iPad and Surface Go)
- Teachers' Standards
- City of London Corporation Acceptable Use of IT Policy
- City of London Corporation Data Protection Policy
- City of London Corporation Employee Code of Conduct
- City of London Corporation Disciplinary Policy
- City of London Corporation Social Media policy

1. Aims

City of London School for Girls aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- 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 and allow our pupils to foster a sense of independence and resilience in the digital age whilst emphasising the opportunities that technology can provide.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- To ensure that online safety is understood to be vital to safeguarding as a whole and be treated with equal focus. It is not a separate issue.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk in line with the Keeping Children Safe in Education 2023:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, 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 scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, **Keeping Children Safe in Education 2023**, and its advice for schools on:

- **Teaching online safety in schools**
- **Preventing and tackling bullying**
- **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),**
- **Education and Inspections Act 2006**
- **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 headmistress 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, 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 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
- Governors should ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies.
- 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 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 headmistress

- The headmistress is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- The safety of all members of the school community, ensuring that sufficient training is in place and accurate reporting procedures.

3.3 The designated safeguarding lead (DSL)

- Details of the school's DSL and DDSL's are set out in our child protection and safeguarding policy as well as relevant job descriptions. The DSL has responsibility to refer more serious breaches where the wellbeing and safety of a child is seriously compromised to the Police, CEOPS, the Local Prevent Coordinator and local Channel panel as appropriate. The DSL understands the unique risks associated with online safety and takes lead responsibility for online safety in school, in particular:
- Supporting the headmistress in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headmistress, Director of Digital Strategy and eSafety Coordinator to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection and behaviour policies, making use of MyConcern and the Incidents log.
- Informing parents what systems the school uses to filter and monitor online use
- Regularly meeting with the Director of Digital Strategy to discuss and review monitoring and filtering systems. Ensuring that the filtering systems are appropriate and proportionate and does not lead to 'overblocking'. These decisions will be done in consultation with the IT department, eSafety Coordinator and eLearning Coordinator.
- Updating and delivering staff training on online safety in conjunction with the eSafety Coordinator, working with external agencies and external services when necessary.
- Providing reports on online safety as part of their safeguarding remit to the headteacher and governing board after being supplied with relevant information by the eSafety Coordinator.
- 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 The eSafety Coordinator

- Ensuring that any online safety incidents are logged that take place through the desktops using IMPERO software and reported to the DSL to be dealt with appropriately in line with the behaviour policy.
- Working with the Deputy Head Pastoral on the promotion of eSafety within the PSHCEE curriculum, ensuring that key topics of online safety are covered that are relevant to the different year groups and to ensure that this is reviewed annually.
- Coordinating the Digital Leaders' Programme to foster independence and leadership when it comes to topics around online safety.
- Provide resources to parents, pupils and staff through online platforms for advice and training.
- Maintain good working knowledge of how generative AI technologies and their misuse could lead to safeguarding threats.
- Maintaining the membership of external organisations to support the online safety provision, keeping updated on the latest findings.

3.5 Technical Staff

Technical staff lead by the IT Manager and the Director of IT are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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. Regularly reviewing the suitability of filtering and monitoring systems with the DSL. Advising DSL of any new potential threats.
- 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 at regular intervals.
- Monitoring the school's ICT systems on a daily basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files or non-age appropriate applications.

3.6 Computer Science Department and eLearning Coordinator

The Head of Computer Science, Computer Science teachers are responsible for:

- Providing a Computer Science curriculum at KS3 which covers content on the safe and responsible use of the internet and digital technologies.
- Recognise the role that generative AI might play in creating online safeguarding (or otherwise) threats and integrate teaching about these into the curriculum.
- The eLearning Coordinator will ensure that digital technologies are up-to-date and pupils and staff are trained to use the mobile devices effectively and responsibly.

3.7 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 and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy and in conjunction with the Behaviour policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour policy and logged on MyConcern.
- 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'.

3.7 Parents

Parents 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 and endorsed this agreement by signature.
- Read all information that is sent by the school with regards to online safety and be responsible for their children's use of technology at home.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- **UK Safer Internet Centre**
- **Childnet International**
- **Internet Matters**
- **Parent Zone**
- **ThinkUKnow**
- **Parent Info**

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.

4. Educating pupils about online safety

4.1 Computer Science Curriculum

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

By the **end of key stage 2**, 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

In the senior school (Key Stage 3), 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
- Understand the legislation that applies to use of technology and the consequences of non compliance
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

Pupils in **Key Stage 5** will be taught:

- The implications of social media and its potential toxicity, cancel culture, performative activism and its impact, managing misinformation and disinformation when it comes to current affairs and considering things through an intersectional lens and being accepting of differing opinions.

By the **end of secondary school**, 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 which 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)
- That generative AI technologies could potentially be behind online agents and the implications that this might have.

4.2 PSHCEE

- The safe use of social media and the internet will also be covered in PSHCEE lessons across the year as well as during form times and assemblies when appropriate.
- The eSafety Coordinator devises a range of lessons across KS3 to KS5 which is reviewed annually to ensure it remains relevant and suitable for the different ages that covers the safe use of the internet and one's digital footprint, cyber-bullying, sharing of data and information including images, videos and sound files as well as cybercrime and implications for mental health.
- Pupils will also have access to relevant guidance which is kept up-to-date as well as be given space to discuss topics of their choice through peer-to-peer sessions (Digital Leaders Programme) when appropriate.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in information evenings, letters or other communications home, and in information via our website, Parent Portal and newsletter.

This policy will also be available to parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headmistress and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the headmistress.

The DSL will let parents know what systems the school uses to filter and monitor online use. The school will also tell parents what their children are asked to do online (for example, sites they need to visit or who they'll be interacting with online, when applicable).

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 intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Behaviour policy.)

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 Tutors will discuss cyber-bullying with their tutor groups as part of the PSHCEE curriculum as well as being raised during Anti-bullying week and Safer Internet Day.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health, citizenship and economic (PSHCEE) 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 and parents are provided with support and advice through their Heads of Years when cyber-bullying issues are raised (see section 11 for more detail).
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the 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 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

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads, laptops and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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 **screening, searching and confiscation**
- UKCIS guidance on **sharing nudes and semi-nudes: advice for education settings working with children and young people**

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/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

CLSG 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 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

CLSG will treat any use of AI to bully pupils in line with our Anti-bullying Policy and Behaviour 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.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors 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, governors and visitors (where relevant) to ensure they comply with the above.

8. Pupils using mobile devices in school

Pupils are allowed to bring mobile phones into school and in Y7 and Y8 are not allowed to use them during lessons or morning break. We acknowledge that 4G can be accessed through these mobile devices and there can be misuse whilst at school. This misuse will be dealt with in line with the Safeguarding and Behaviour policies.

Pupils are issued with a school iPad to use in lessons but only when instructed by their teachers. iPads and for Sixth Form their own personal devices can only use the internet on site using the school internet which has appropriate filters organised by the IT Department. School iPads are also monitored in a similar fashion. CS pupils are issued with a laptop for their studies.

Pupils understand and follow the school's eSafety and acceptable usage policies and in turn are responsible for using the school IT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given access to school systems. (Parents can find copies of these policies for iPad and Surface Go in the policy section of My School Portal.)

As part of their education pupils understand the importance of:

- reporting abuse, misuse or access to inappropriate materials and know how to do so
- adopting good eSafety practice when using digital technologies out of school and realise that the school's eSafety policy also covers their actions out of school, if related to their membership of the school.

Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations through their subject lessons.
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.

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)
- Making sure the device locks if left inactive for a period of time

- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use and ensure that they are up-to-date with eSafety matters and eSafety Policy.

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

All staff members will take appropriate steps to support pupil's use of technology in lessons. This includes, but is not limited to:

- Embed key advice with regards to the use of the internet through their lessons
- Monitoring pupils' use of technology within the classroom
- Report any misuse to the Head of Year/DSL.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet or their school issued iPads, Surface or BYOD, we will follow the procedures set out in our 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 disciplinary procedures. 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 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).

All staff read Keeping Children Safe in Education annually and through discussions and completion of any quizzes the school deem necessary, demonstrate an understanding of their obligations and training.

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
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- 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 or video/audio, to those who don't want to receive such content

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 the risks up
- 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 DDSLs 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 and Safeguarding and Child Protection policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety through MyConcern as well as an incident report log being kept for any misuse on the IT systems. This monitoring will ensure we are fulfilling our Prevent duties as well.