City of London School Digital Safety Policy

0. Review of Policy

0.1 This policy will be reviewed on an annual yearly basis (or more regularly where required) prior to approval by the Board of Governors.

Policy last reviewed by:	Alice Martineau (Deputy Head (Pastoral))
Date last reviewed:	May 2025 (changes as shown)
Approved for Governors by:	Board of Governors
Date approved:	19 June 2025

1. Introduction

1.1 New technologies have become integral to the lives of young people in today's world. The internet and other digital information and communications technologies are powerful tools, which offer new opportunities for everyone. These technologies have enormous benefits: stimulating discussion, promoting creativity, enabling connectivity and enhancing learning. At home, technology is changing the way young people live and manage their time as well as the activities in which they choose to engage. These trends are set to continue.

1.2 However, developing technologies also bring risks and potential dangers, including:

- Access to illegal, harmful or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data
- The risk of being subject to grooming by those with whom contact has been made online
- The risk of coming into contact with extremist material posted with the aim of radicalisation
- The sharing / distribution of personal images without consent or knowledge
- Inappropriate contact / communication with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information, particularly with regard to concerns about 'fake news'

- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive or addictive use which may impact on social and emotional development and/or learning

1.3 This policy should be read in conjunction with the following School policies:

- The School Standards, Rules and Regulations
- The Acceptable Use Policy for Staff
- The Safeguarding and Child Protection Policy and the Safeguarding Code of Conduct
- The Policy on Taking, Using and Storing images of Children and Young People
- The Data Protection Policy
- The Anti-Bullying Policy
- The Mental Health Policy
- The Behaviour Policy

1.4 This policy has regard to Part 3 (Welfare, health and safety of pupils), Paragraphs 7 (Safeguarding) and 10 (Bullying) of the Independent School Standards Regulations.

1.5 This policy should be read in conjunction with the DfE document *Generative artificial intelligence in education*, P6 Minimising harm.

2. Aims of the Policy

2.1 The aims of the Digital Safety policy are to:

- promote the welfare and safeguarding of pupils and staff at the School
- ensure that pupils are ICT literate and can use the relevant facilities to ensure that their educational provision is enhanced to the maximum
- promote responsible and effective use of electronic communication (including the use of the internet, social media, mobile phones and digital technology)
- educate pupils and staff about the risks, responsibilities and potential criminal implications involved in the use of technology
- raise awareness of and counter instances of cyber-bullying, including bullying via text message, instant-messenger services and social network sites (such as Facebook, Twitter, Instagram, SnapChat, etc.), email, and images or videos posted on the internet or spread via mobile phones

3. Management of the Policy

3.1 This Policy has been written by the School and builds on the advice of a range of legislation and advice from government and local authority. The Designated Safeguarding Lead (DSL) will serve as the Digital Safety Coordinator.

The following measures are in place to support this policy:

- The induction of new pupils and staff
- Regular training for all staff
- The PSHEE, form time and assembly programmes, and Schemes of Work developed in collaboration with the Director of Digital strategy
- Specific guidance to exam classes about plagiarism
- Specific Parents' Pastoral Evenings
- The Parents' Forum
- Induction of new parents and refreshers for existing parents on the use of these platforms
- Regular monitoring of pupils' activity across the network and internet (using Senso.cloud and Lightspeed)

4. Access to the Internet

4.1 The School will do all it can to monitor access to the internet via the School network. Access to the School internet has been designed expressly for the use of pupils and includes filtering appropriate to the age of the pupils, including terms for the Prevent Duty.

4.2 Access to the internet for pupils and staff is governed by the School's Acceptable Use Policy for Staff and Acceptable Use Policy for Pupils, which lay down the framework within which the School network can be accessed and gives clear guidelines about pupil and staff online behaviour in relation to the internet, social media, and the use of the School network. Pupils and staff are granted access to the internet by agreeing to the terms of the relevant Acceptable Use Policy. Any pupil or member of staff who breaches these terms may have access to the internet withdrawn.

4.3 A regular analysis is conducted of the pupils' internet usage which is shared with Heads of Year and the Deputy Head Pastoral and is used to identify potential trends or problems.

4.4 The School will ensure that guidance about the copying and subsequent use of internet-derived materials by pupils and staff complies with copyright law, and pupils will be taught to be critically aware of the materials they read. They will also be taught to acknowledge the sources of information used.

4.5 The security of the School information systems will be reviewed regularly with e-Security measures updated on a regular basis.

5. Email

5.1 Pupils and staff are inducted into the appropriate use of email and there is clear guidance in the Acceptable Use Policies about what is, and is not, acceptable in terms of e-mail communication. Any inappropriate email must be reported to the pupil's Form Tutor immediately.

5.2 Transparency, openness and appropriate professional purpose must underpin all academic and pastoral interaction with pupils via electronic and digital means.

5.3 The Safeguarding Code of Conduct makes clear that pupils and staff may only communicate via School email (i.e. accounts ending with @cityoflondonschool.org.uk or @cityschools.org.uk).

6. Social Media

6.1 Staff are bound by the City of London Corporation's Social Media Policy.

6.2 Pupils and staff should follow the following guidelines regarding the use of Social Media:

- Pupils and staff must always keep their social media profiles on the highest levels of privacy and to update privacy settings regularly
- Pupils and staff must never to give out personal details of any kind which may enable them or their location to be identified
- Staff must avoid posts or comments that refer to specific matters related to the School and / or members of its community on any social media sites, and to be mindful of their professional reputation and the reputation of the School whilst conducting any online activity
- Staff must not to run social network spaces for pupils' use on a personal basis; any sharing of homework, lesson plans, etc. should be done via Teams or OneNote.
- Staff must not allow any current pupil (including a recent leaver, i.e. in the school year immediately following the year of their leaving the School) to be their 'friend' or 'follower' on any social media site
- Pupils, staff and parents are regularly updated with advice and information concerning new social media apps, changes in social media protocols (for example Snapchat's location finder) and trends in online behaviour
- Pupils and staff are regularly reminded of the risks posed by adults or young people who use the internet and social media to bully, groom, abuse or radicalise other people

7. Cyber-Bullying

7.1 The internet and social networking sites must not be used to intentionally or deliberately hurt, humiliate, slander or defame another person. Pupils are made aware that actions in this regard undertaken outside of School may also contravene School policies and so may be subject to School sanctions (in the first instance). The same sanctions will apply to incidents of cyber-bullying as would apply to any other form of bullying.

7.2 The Anti-Bullying Policy gives further guidance on cyber-bullying and a summary is displayed on the noticeboard of every classroom.

8. Sharing of nudes and semi-nudes (formerly sexting)

8.1 The UK Council for Internet safety (UKCIS) publishes non-statutory guidance[1] on managing incidents of sharing of nudes and semi-nudes by under-18s. The UKCIS guidance is non-statutory, but should be read alongside *Keeping Children Safe in Education (KCSIE)*[2], and it should be followed unless there is a good reason not to do so.

8.2 The sharing of nudes and semi nudes is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. The UKCIS guidance uses the terminology 'youth-produced sexual imagery'. This is imagery that is being created by under-18s themselves and involves still photographs, video and / or streaming. In the guidance, this content is described as sexual and not indecent. The term 'indecent' is subjective and has no specific definition in UK law.

8.3 Incidents covered by the guidance:

- A person under 18 creates a sexual image of themself and shares it with another person under 18.
- A person under 18 shares an image of another under-18 with another person under 18 or an adult.
- A person under 18 is in possession of sexual imagery created by another person under 18.

8.4 Incidents not covered by the guidance:

- Under-18s sharing adult pornography.
- Under-18s sharing sexual texts without sexual imagery.
- Adults sharing sexual imagery of under-18s. (This is child sexual abuse and must always be reported to police.)

8.5 See Appendix 1 for how to respond to incidents of youth produced sexual imagery.

9. Mobile phones and portable electronic devices

[1] See https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-how-to-respond-to-an-incident-overview

9.1 As a commuting school in the centre of London, the School recognises that pupils are likely be in possession of a mobile device for the journey to and from School and in the event of an emergency or critical incident.

9.2 Pupil use of mobile phones and portable electronic devices as outlined in the School Standards (Rules and Regulations) and Acceptable Use Policy (Pupils).

9.3 Pupils and staff are made aware that the guidelines that apply to the use of the School network also apply to any handheld communication device that is brought into School. Nothing that is inappropriate or potentially illegal should be downloaded or saved onto these devices, and all pupils and staff should be aware of the possible criminality of transmitting such material.

9.4 Where information is accessed on personal devices, including through the device owner's service provider, whether or not such use is permitted, such devices may be confiscated and examined (in line with the Pupil Searches and Confiscation of Pupils' Belongings Policy). The School may require staff to conduct searches of personal accounts or devices if they are suspected to have been used in contravention of this policy.

10. Photography / Video recording / Audio recording

10.1 Pupils and staff should follow the following guidelines regarding the use of Social Media:

- Any recording taken of a pupil must be for legitimate educational reasons. The validity and necessity of such a recording must be transparent, obvious and approved in advance by the member of staff's line-manager or the DSL
- Pupil consent must always be obtained; recordings must never be clandestine
- Care must be taken if recording images of pupils in clothing other than normal school dress (e.g. sports kit or costume drama). It is <u>never</u> acceptable to record images where pupils may not be fully dressed (e.g. backstage in drama productions or changing rooms or sports venues)
- Staff should never use their own personal mobile or digital device to capture images of pupils. In departments where photography of pupils for educational purposes is relatively commonplace, for example in Music, Sports and Drama, departmental devices have been issued.

10.2 Copies of any recording taken of a pupil must not be made, nor distributed or shared

10.3 Further information is given in the School's Taking, Using and Storing images of Children and Young People Policy.

11. Complaints

11.1 Complaints about serious digital or internet misuse will normally be handled in the first instance by the Head of Section and will be referred to the Deputy Head Pastoral and / or Senior Deputy Head.

11.2 All incidents of serious internet misuse must be recorded and passed on the Deputy Head Pastoral and Senior Deputy Head.

12. Child Protection and Safeguarding

12.1 Cyber-bullying, grooming, radicalisation, sextortion and the sharing of nudes and semi-nudes are serious safeguarding issues. As a result, any concerns regarding pupils and their digital activities should be discussed with the DSL before taking action.

12.2 Staff, parents and pupils should be aware that School email and internet usage (including through School Wi-Fi) will be monitored for Safeguarding and Conduct purposes, and both web history and school email accounts may be accessed where necessary for a lawful purpose, including serious conduct or welfare concerns, concerns regarding extremism, and for the protection of others.

Annex 1: Response to incidents of youth produced sexual imagery

Guidance from: *UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people*[3]

1.1 The response should be guided by the 'principle of proportionality'. 'The primary concern at all times should be the welfare and protection of the young people involved.' (*UKCIS: **Sharing nudes and semi-nudes: advice for education settings working with children and young people.)***

1.2 **The Law**

Making, possessing, and distributing any imagery of someone under 18 which is indecent is illegal. This includes imagery of yourself if you are under 18. 'Indecent' is not definitively defined in law, but images are likely to be considered indecent if they depict:

- nude or semi-nude sexual posing (e.g. displaying genitals and/or breasts or overtly sexual images of young people in their underwear)
- someone nude or semi-nude touching themselves in a sexual way
- any sexual activity involving a child
- someone hurting someone else sexually
- sexual activity that includes animals

The law criminalising indecent images of children was created to protect children and young people from adults seeking to sexually abuse them or gain pleasure from their sexual abuse. It was not intended to criminalise children and young people. The law was also developed long before mass adoption of the internet, mobiles and digital photography.

Despite this, children and young people who share nudes and semi-nudes of themselves, or peers, are breaking the law.

However, children and young people should not be unnecessarily criminalised. Children and young people with a criminal record face stigma and discrimination in accessing education, training, employment, travel and housing and these obstacles can follow them into adulthood.

The NPCC has made it clear that incidents involving sharing nudes and semi-nudes should have an immediate focus on safeguarding children.

1.3 **Crime recording**

When an incident of sharing nudes and semi-nudes is reported to police, they are obliged, under the Home Office Counting Rules and National Crime Recording Standards, to record the incident on their crime systems. The incident will be listed as a 'crime' and the child or young person involved may be listed in relation to it.

[3] See https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

This is not the same as having a criminal record.

Once an incident is reported to the police, they will investigate and decide on an appropriate outcome.

If an incident is found to have abusive and/or aggravating factors, the child or young person may receive a caution or conviction.

To mitigate the risk of children and young people being negatively impacted, the police are able to record the outcome of an investigation using an outcome 21 code should an incident be found to be non-abusive and have no evidence of any of the following:

exploitation
grooming
profit motive
malicious intent (e.g. extensive or inappropriate sharing e.g. uploading onto a pornographic website)
persistent behaviour
The outcome 21 code, launched in 2016, helps to formalise the discretion available to the police when handling crimes such as the sharing of nudes and semi-nudes.

1.4 Handling incidents

- When an incident involving nudes and semi-nudes comes to the attention of any member of staff in an education setting:
- the incident should be referred to the DSL (or equivalent) as soon as possible
- the DSL (or equivalent) should hold an initial review meeting with appropriate staff. This may include the staff member(s) who heard the disclosure and the safeguarding or leadership team who deal with safeguarding concerns
- there should be subsequent interviews with the children or young people involved (if appropriate)
- parents and carers should be informed at an early stage and involved in the process in order to best support the child or young person unless there is good reason to believe that involving them would put the child or young person at risk of harm

- a referral should be made to children's social care and/or the police immediately if there is a concern that a child or young person has been harmed or is at risk of immediate harm at any point in the process Once a DSL has enough information, the decision should be made to deal with the matter in school or to refer it to the police or to social care. All information and decision-making should be recorded in line with school policy. If the incident has been dealt with in school, a further review should be held to assess risks.

1.5 Assessing the risks once the images have been shared

The circumstances of incidents can vary widely. If at the initial review stage a decision has been made not to refer to police and/or children's social care, the DSL (or equivalent) should

conduct a further review (including an interview with any child or young person involved) to establish the facts and assess the risks, referring back to any relevant assessment tools.

When assessing the risks and determining whether a referral is needed, the following should be also considered:

Why was the nude or semi-nude shared? Was it consensual or was the child or young person put under pressure or coerced?

Has the nude or semi-nude been shared beyond its intended recipient? Was it shared without the consent of the child or young person who produced the image?

Has the nude or semi-nude been shared on social media or anywhere else online? If so, what steps have been taken to contain the spread?

How old are any of the children or young people involved?

Did the child or young person send the nude or semi-nude to more than one person?

Do you have any concerns about the child or young person's vulnerability?

Are there additional concerns if the parents or carers are informed?

- These questions will help the DSL (or equivalent) decide whether a child or young person is at risk of harm, in which case a referral will be appropriate, whether additional information or support is needed from other agencies or whether the education setting can manage the incident and support any child or young person directly. DSLs (or equivalent) should always use their professional judgement in conjunction with that of their colleagues to assess incidents.

1.6 Viewing images

- Avoid viewing youth-produced sexual imagery. Instead, respond to what you have been told the image contains.
- If such imagery is viewed, discuss with the Designated Safeguarding Lead **immediately.**
- **Never copy, print, or share the image (it is illegal to do so).**
- View the image with another member of staff present.
- Record the fact that the images were viewed, along with reasons for doing so and who was present. Sign and date this record.

See section 2.10 of *UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people*[4] *for further, detailed guidance relating to viewing images*

[4] See https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

1.7 Deleting images (from devices and social media)

If the school has decided that other agencies do not need to be involved, then consideration should be given to deleting nudes and semi-nudes from devices and online services to limit any further sharing.

In most cases, children and young people should be asked to delete the imagery and to confirm that they have deleted them. They should be given a deadline for deletion across all devices, online storage or social media sites. They should be reminded that possession of nudes and semi-nudes is illegal. They should be informed that if they refuse or it is later discovered they did not delete the imagery, they are continuing to commit a criminal offence and the police may become involved.