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:	August 2021 (changes as shown)
Approved for Governors by:	Board of Governors
Date approved:	8 December 2021

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.

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 City of London Police recommended *Get Safe Online* advice[1] and government guidance, including City and Hackney Safeguarding Children's Board *Safeguarding in the Context of Access to Technology and Use of Social Media*, 2017[2]. The Designated Safeguarding Lead (DSL) will serve as the Digital Safety Coordinator.

The following measures are in place to support this policy:

- The DSL has completed CEOP Thinkuknow Training
- The induction of new pupils and staff
- Regular training for all staff
- The PSHE, form time and assembly programmes, and the IT&C Departmental Scheme of Work
- Guidance during any academic lesson about use of the internet
- Specific guidance to exam classes about plagiarism
- Specific Parents' Pastoral Evenings
- The Parents' Forum
- School membership to Parentzone which included free online training
- Induction of new parents on the use of Parentzone
- Regular monitoring of pupils' activity across the network and internet (using Sophos, 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 recommended by Surrey Police[3].

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.

[1] See www.getsafeonline.org

[2] See http://www.chscb.org.uk/wp-content/uploads/2017/09/CHSCB-Safeguarding-in-the-Context-of-Access-to-Technology-and-Use-of-Social-Media-Handbook-digital-version.pdf

[3] See https://www.surrey.police.uk/advice/protect-yourself-and-others/counter-terrorism/

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).

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 are advised to always keep their social media profiles on the highest levels of privacy and to update privacy settings regularly
- Pupils and staff are advised never to give out personal details of any kind which may enable them or their location to be identified
- Staff are advised to 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 are advised not to run social network spaces for pupils' use on a personal basis; any sharing of homework, lesson plans, etc. should be done via the School's internal Virtual Learning Environment / Pupil Intranet
- Staff are advised not to 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.

7.3 There Anti-Bullying Handbook is distributed to all parents at the beginning of each academic year and to all pupils in the first Form Time of each academic year.

8. Sexting

8.1 In August 2016, the UK Council for Child Internet Safety (UKCCIS) published non-statutory guidance[4] on managing incidents of sexting by under-18s. The UKCCIS guidance is non-statutory, but should be read alongside *Keeping Children Safe in Education (KCSIE)*[5], and it should be followed unless there is a good reason not to do so.

8.2 There is no clear definition of 'sexting'. The UKCCIS 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

[4] See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf

[5] See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/550499/Keeping_children_safe_in_education_Part_1.pdf

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

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

9.2 Pupils may use 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. Pupils and staff should follow the following guidelines regarding the use

1 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 never acceptable to record images where pupils may not be fully dressed (e.g. backstage in drama productions or changing rooms or sports venues)
- It is best practice to use designated School IT equipment to make or show recordings (or any other relevant material for educational purposes)
- 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 Year 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. Cyber-bullying, grooming, radicalisation and sexting are safeguarding

1 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: *UKCCIS Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People*, 2016[6]

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.' (*UKCCIS Sexting in schools and colleges: responding to incidents and safeguarding young people*, p.8).

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:

- a naked young person
- a topless girl
- an image which displays genitals
- sex acts including masturbation
- indecent images may also include overtly sexual images of young people in their underwear

These laws were not created to criminalise young people but to protect them. Although sharing sexual images of themselves is illegal and risky, it is often the result of curiosity and exploration. Young people need education, support, and safeguarding, not criminalisation.
The National Police Chiefs' Council (NPCC) is clear that "youth-produced sexual imagery should be primarily treated as a safeguarding issue."
Schools may respond to incidents without involving the police. (However, in some circumstances, the police must always be involved.)

3. Crime recording

When the police are notified about youth-produced sexual imagery, they must record this as a crime. The incident is listed as a crime, and the young person is the suspect. This is, however, not the same as a criminal record. Every crime reported to the police must have an outcome code. The NPCC, Home Office and the Disclosure and Barring Service (DBS) have agreed a new outcome code for youth-produced sexual imagery: **Outcome 21**. This outcome code allows the police discretion not to take further action if it is not in the public interest, even though there is enough evidence to prosecute.
Using this outcome code is likely, although not impossible, to mean the offence would not appear on a future Enhanced DBS check, as that disclosure is a risk-based decision. Schools can be assured that the police have the discretion they need not to adversely impact young people in the future.

[6] See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf

1.4 Handling incidents

- Refer to the Designated Safeguarding Lead (DSL)
- The DSL will meet with the young person / people involved
- Do not view the image unless it is unavoidable (see *Viewing Images* below); confiscate the device, switch off the device and place the device in a sealed (and signed and dated) envelope.
- Discuss with parents, unless there is an issue where that's not possible
- If there is any concern the young person is at risk of harm, social care or the police should be contacted

Always refer to the police or social care if incident involves:

- an adult
- coercion, blackmail, or grooming
- concerns about capacity to consent (e.g. if the young person has SEN)
- images show atypical sexual behaviour for the child's developmental stage
- violent acts are depicted
- image shows sex acts and includes a child under 13
- a young person at risk of immediate harm as a result of the disclosure (for example, self-harm or suicide)

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

When assessing the risks (to the young person) when an image has been shared, the following points should be considered:

- Has it been shared with the knowledge of the young person?
- Are adults involved in the sharing?
- Was there pressure to make the image?
- What is the impact on those involved?
- Does the child or children have additional vulnerabilities?
- Has the child taken part in producing sexual imagery before?

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.

17. Deleting images (from devices and social media)

If the school has decided that involving other agencies is not necessary, consideration should be given to deleting the images. It is recommended that pupils are asked to delete the images themselves and confirm they have done so. This should be recorded, signed, and dated. Any refusal to delete the images should be treated seriously, reminding the pupil that possession is unlawful.