CATHEDRAL SCHOOLS TRUST

Online Safety Policy

It is the responsibility of all Cathedral Schools Trust employees, governors and volunteers to familiarise themselves with the contents of all Trust policies and any amendments hereafter.

Cathedral Schools Trust
[Name of School]

May 2025

Contents

1	Aims	2
2	Scope and application	3
3	Regulatory framework	3
4	Publication and availability	5
5	Definitions	5
6	Responsibility statement and allocation of tasks	6
7	Role of staff and Parents	7
8	Filtering and Monitoring	11
9	Access to the Academy's technology	12
10	Procedures for dealing with incidents of misuse	15
11	Education	17
12	Training	19
13	Mobile phones	22
14	Cybercrime	22
15	Risk assessment	23
16	Record keeping	24
17	Version control	24

1 Aims

1.1 This is the online safety policy of [· name of school] (**Academy**).

1.2 The aim of this policy is to promote and safeguard the welfare of all pupils through the implementation of an effective online safety strategy which empowers the Academy to:

1.2.1 protect the whole Academy community from [potentially] illegal, inappropriate and harmful content or contact;

1.2.2 educate the whole Academy community about their access to and use of technology;

1.2.3 establish effective mechanisms and processes to identify, intervene in and escalate concerns where appropriate; and

1.2.4 promote a whole school culture of openness, safety, equality and protection.

1.3 This policy forms part of the Academy's whole school approach to promoting child safeguarding and wellbeing, which involves everyone at the Academy and seeks to ensure that the best interests of pupils underpins and is at the forefront of all decisions, systems, processes and policies.

1.4 Online safety is a running and interrelated theme throughout the devising and implementation of many of the Academy's policies and procedures including its Safeguarding and child protection policy and procedures and careful consideration has been given to ensure that it is also reflected in the Academy's curriculum, teacher training and any parental engagement, as well as the role and responsibility of the Academy's Designated Safeguarding Lead (**DSL**) (and any deputies).

1.5 Although this policy is necessarily detailed, it is important that our safeguarding related policies and procedures are transparent, clear and easy to understand for staff, pupils, parents and carers. The Academy welcomes feedback on how we can continue to improve our policies.

2 Scope and application

2.1 This policy applies to the whole Academy [· including the Early Years Foundation Stage (**EYFS**)].

2.2 This policy applies to all members of the Academy community, including staff and volunteers, pupils, Parents and visitors, who have access to the Academy's technology whether on or off Academy premises, or otherwise use technology in a way which affects the welfare of other pupils or any member of the Academy community or where the culture or reputation of the Academy is put at risk.

3 Regulatory framework

3.1 This policy has been prepared to meet the Academy's responsibilities under:

3.1.1 Education (Independent School Standards) Regulations 2014;

3.1.2 [*EYFS only/delete if not relevant*] **EYFS statutory framework for group and school-based providers (DfE, January 2024);**

3.1.3 Education and Skills Act 2008;

3.1.4 Children Act 1989;

3.1.5 Childcare Act 2006;

3.1.6 Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR); and

3.1.7 Equality Act 2010.

3.2 This policy has regard to the following guidance and advice:

3.2.1 Keeping children safe in education (DfE, September 2024) (**KCSIE**);

3.2.2 Working together to safeguard children (HM Government, July 2018, updated July 2022);

3.2.3 Preventing and tackling bullying (DfE, July 2017);

3.2.4 Sharing nudes and semi-nudes: advice for education settings working with children and young people (Department for Digital, Culture, Media & Sport (**DfDCMS**) and UK Council for Internet Safety (**UKCIS**), December 2020);

3.2.5 Prevent duty guidance for England and Wales (Home Office, **October 2023, in force on 31 December 2023**);

3.2.6 Channel duty guidance: protecting people susceptible to radicalisation (Home Office, October 2023);

3.2.7 Searching, screening and confiscation: advice for schools (DfE, July 2022, in force from September 2022);

3.2.8 Behaviour in schools: advice for headteachers and school staff **(DfE, February 2024);**

3.2.9 Safeguarding children and protecting professionals in early years settings: online safety considerations (UK Council for Internet Safety, February 2019);

3.2.10 Meeting digital and technology standards in education **(DfE, March 2023);**

3.2.11 Teaching online safety in schools (DfE, January 2023);

3.2.12 Relationships education, relationships and sex education (RSE) and health education guidance (DfE, September 2021);

3.2.13 Harmful online challenges and online hoaxes (DfE, February 2021);

3.2.14 Online safety guidance if you own or manage an online platform (DfDCMS, June 2021);

3.2.15 A business guide for protecting children on your online platform (DfDCMS, June 2021);

3.2.16 Online safety in schools and colleges: questions from the governing body (UKCIS, October 2022);

3.2.17 Online safety audit tool (UKCIS, October 2022);

3.2.18 Appropriate filtering for education settings (UKCIS, May 2023);

3.2.19 Appropriate monitoring for schools (UKSIC, May 2023); and

3.2.20 Online safety self-review tool for schools, 360safe.

3.2.21 Mobile phones in schools (DfE, February 2024)

3.2.22 Meeting digital and technology standards in education (DfE, March 2025)

3.3 The following Academy policies, procedures and resource materials are relevant to this policy:

3.3.1 Acceptable use policy for pupils

3.3.2 IT acceptable use policy within CST Employment Manual

3.3.3 Safeguarding and Child Protection Policy

3.3.4 Anti-bullying policy

3.3.5 Behaviour policy

3.3.6 [• School rules;] [• Statement of behaviour principles;]

3.3.7 [• Risk assessment policy for pupil welfare;]

3.3.8 Whistleblowing policy

3.3.9 Data protection policy

3.3.10 Information security incident procedure

3.3.11 [• Use of mobile phones and cameras in the early years foundation stage (EYFS) Setting: EYFS only.]

3.3.12 [• Relationships education / Relationships and sex education policy].

4 Publication and availability

4.1 This policy is published on the School website.

4.2 This policy is available in hard copy on request.

4.3 A copy of the policy is available for inspection from the school office during the school day.

4.4 This policy can be made available in large print or other accessible format if required.

5 Definitions

5.1 Where the following words or phrases are used in this policy:

5.1.1 References to the **Proprietor** are references to Cathedral Schools Trust, the **Academy Trust**.

5.1.2 Reference to staff includes all those who work for or on behalf of the Proprietor, regardless of their employment status, including contractors, supply staff, volunteers, Trustees and Governors unless otherwise indicated.

5.1.3 Senior Leadership Team (SLT) comprises of the Headteacher, and DSL and [• state if others].

5.1.4 In considering the scope of the Academy's online safety strategy, the Academy will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as **technology**).

5.1.5 References to **Parent** or **Parents** means the natural or adoptive Parents of the pupil (irrespective of whether they are or have ever been married, with whom the pupil lives, or whether they have contact with the pupil) as well as any person who is not the natural or adoptive Parent of the pupil, but who has care of, or Parental responsibility for, the pupil (e.g. foster carer / legal guardian).

6 Responsibility statement and allocation of tasks

6.1 The Proprietor has overall responsibility for all matters which are the subject of this policy and for approving and reviewing its effectiveness.

6.2 The Proprietor is required to ensure that all those with leadership and management responsibilities at the Academy actively promote the well-being of pupils. The adoption of this policy is part of the Proprietor's response to this duty.

6.3 The Proprietor is aware of its duties under the Equality Act 2010 and the requirement under S.149 of the Equality Act 2010 to meet the Public Sector Equality Duty. This means in carrying out its functions, the Proprietor is required to have due regard to the need to:

6.3.1 eliminate discrimination and other conduct that is prohibited by the Act;

6.3.2 advance equality of opportunity between people who share a protected characteristic and people who do not share it; and

6.3.3 foster good relations across all characteristics - between people who share a protected characteristic and people who do not share it.

6.4 To ensure the efficient discharge of its responsibilities under this policy, the Proprietor has allocated the following tasks:

Task	Allocated for	When / frequency of review
Keeping the policy up to date and compliant with the law and best practice	**CST Leadership Team**	**As required, and at least termly**
Monitoring the implementation of the policy (including the record of incidents involving the use of technology and the logs of internet activity and sites visited), relevant risk assessments and any action taken in response and evaluating effectiveness	**Headteacher**	**As required, and at least termly**
Online safety	**DSL**	**As required and at least annually**
Reviewing filtering and monitoring provision	**SLT, DSL and IT service provider and responsible governor**	**As required, and at least annually**
Seeking input from interested groups (such as pupils, staff, Parents) to consider improvements to the	**Headteacher**	**As required, and at least annually**

Academy's processes under the policy		
Formal annual review	**Proprietor**	**As a minimum annually, and as required**
Overall responsibility for content and implementation	**Proprietor**	**As a minimum annually**

7 Role of staff and Parents

7.1 Academy Trust

7.1.1 The Academy Trust as Proprietor has overall responsibility for safeguarding arrangements within the Academy, including the Academy's approach to online safety and the use of Technology within the Academy.

7.1.2 The Academy Trust is required to ensure that all those with leadership and management responsibilities at the Academy actively promote the well-being of pupils. The adoption of this policy is part of the Academy response to this duty.

7.1.3 The Nominated Safeguarding Trustee is the senior board level lead with leadership responsibility for the Academy's safeguarding arrangements, including the Academy's online safety procedures, on behalf of the Academy Trust.

7.1.4 The Academy Trust will undertake an annual review of the Academy's safeguarding procedures and their implementation, which will include consideration of the effectiveness of this policy and related policies in meeting the aims set out in paragraph 1.2 above.

7.2 Headteacher and Senior Leadership Team

7.2.1 The Headteacher has overall executive responsibility for the safety and welfare of members of the Academy community. This includes a specific responsibility to ensure that the Academy has an effective filtering policy in place that is applied and updated on a regular basis.

7.2.2 The DSL is the senior member of staff from the Academy's leadership team with lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems in place in school.

7.2.3 The responsibility of the DSL includes:

a) managing safeguarding incidents involving the use of technology in the same way as other safeguarding matters, in accordance with the CST Safeguarding and child protection policy and procedures;

b) ensuring all staff are appropriately trained and aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents;

c) working with the ICT Director (see below) in monitoring technology uses and practices across the Academy and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.;

d) overseeing and acting on: filtering and monitoring reports, safeguarding concerns and checks to filtering and monitoring systems;

e) regularly monitoring the technology incident log maintained by the ICT Director;

f) regularly updating other members of the Academy's Senior Leadership Team and the Proprietor on the operation of the Academy's safeguarding arrangements, including online safety practices;

g) providing training and advice for governors / staff / parents / carers / learners;

h) promoting an awareness of and commitment to online safety education / awareness raising across the Academy and beyond.

7.3 ICT Director

7.3.1 The ICT Director, together with their team, is responsible for the effective operation of the Academy's filtering system so that pupils and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the Academy's network.

7.3.2 The ICT Director is responsible for ensuring that:

1. the Academy's technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;

2. the user may only use the Academy's technology if they are properly authenticated and authorised;

3. maintaining filtering and monitoring systems, providing filtering and monitoring reports and completing actions following concerns or checks to systems;

4. the risks of pupils and staff circumventing the safeguards put in place by the Academy are minimised;

5. the use of the Academy's technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and

6. monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the Academy's network and maintain logs of such usage.

7.3.3 [*Include details, or cross-refer to separate written protocols, setting out technical provision and safeguards in place to filter and monitor inappropriate content and to alert the Academy to safeguarding issues*] to input detail on the provision in each school (e.g. netsweeper) as detailed in 'Filtering and Monitoring - How CST meet the standard' - any queries please check with ICT Director.

7.3.4 The ICT Director will report regularly to the Senior Leadership Team on the operation of the Academy's technology. If the ICT Director has concerns about the functionality, effectiveness, appropriateness or use of technology within the Academy, including of the monitoring and filtering systems in place, they will escalate those concerns promptly to the Academy's DSL.

7.3.5 The ICT Director is responsible for maintaining the technology incident log (a central record of all serious incidents involving the use of technology) and bringing any matters of safeguarding concern to the attention of the DSL in accordance with the CST Safeguarding and child protection policy and procedures.

7.4 **All staff**

7.4.1 All staff have a responsibility to act as good role models in their use of technology and to share their knowledge of the Academy's policies and of safe practice with the pupils.

7.4.2 Staff are expected to adhere, so far as applicable, to each of the policies referenced in this policy.

7.4.3 Training for staff includes online safety which, amongst other things, includes an understanding of filtering and monitoring provisions in place, how to manage them effectively, how to escalate concerns when identified and any particular expectations or responsibilities in relation to filtering and monitoring.

7.4.3 All staff are aware that technology can play a significant part in many safeguarding and wellbeing issues and that pupils are at risk of abuse online as well as face-to-face. Staff are also aware that, sometimes, such abuse will take place concurrently online and during a pupil's daily life.

7.4.4 Staff are expected to be alert to the possibility of pupils abusing their peers online and to understand that this can occur both inside and outside of school. Examples of such abuse can include:

the sending of abusive, harassing and misogynistic messages;

the consensual and non-consensual sharing of indecent images and videos (especially around group chats), which is sometimes known as sexting or youth produced sexual imagery;

the sharing of abusive images and pornography to those who do not wish to receive such content;

cyberbullying.

7.4.5 Staff are also aware that many other forms of abuse may include an online element. For instance, there may be an online element which:

facilitates, threatens and / or encourages physical abuse;

facilitates, threatens and / or encourages sexual violence; or

is used as part of initiation / hazing type violence and rituals.

7.4.6 It is important that staff recognise the indicators and signs of child-on-child abuse, including where such abuse takes place online, and that they know how to identify it and respond to reports. Staff must also understand that, even if there are no reports of child-on-child abuse at the Academy, whether online or otherwise, it does not mean that it is not happening; it may simply be the case that it is not being reported.

7.4.7 It is important that staff challenge inappropriate behaviours between peers and do not downplay certain behaviours, including sexual violence and sexual harassment, as "*just banter*", "*just having a laugh*", "*part of growing up*" or "*boys being boys*" as doing so can result in a culture of unacceptable behaviours, an unsafe environment for children and, in a worst case scenario, a culture that normalises abuse.

7.4.8 The Academy has a **zero tolerance approach** towards child-on-child abuse (including in relation to sexual violence and sexual harassment) and such behaviour is never acceptable and will not be tolerated. The Academy will treat any such incidents as a breach of discipline and will deal with them under the Academy's Behaviour policy and also as a safeguarding matter under the CST Safeguarding and child protection policy and procedures.

7.4.9 Staff have a responsibility to report any concerns about a pupil's welfare and safety to the DSL and in accordance with this policy and the CST Safeguarding and child protection policy and procedures. If staff have any concerns regarding child-on-child abuse or if they are

unsure as to how to proceed in relation to a particular incident, they should **always speak to the DSL in all cases**.

7.5 Parents

7.5.1 The role of Parents in ensuring that pupils understand how to stay safe when using technology is crucial. The Academy expects Parents to promote safe practice when using technology and to:

(a) support the Academy in the implementation of this policy and report any concerns in line with the Academy's policies and procedures;

(b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and

(c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

7.5.2 If Parents have any concerns or require any information about online safety, they should contact the DSL. [*Include details of any online reporting mechanism*]

8 Filtering and Monitoring

8.1 Whilst considering their responsibility to safeguard and promote the welfare of pupils and provide them with a safe environment in which to learn, the Proprietor will do all it reasonably can to limit pupil's exposure to risks from the Academy's IT system. As part of this process the Academy has appropriate filtering and monitoring systems in place and regularly reviews their effectiveness.

8.2 The Academy will implement DfE compliant filtering and monitoring standards to limit exposure to online risks ensuring that it:

a) identifies and assigns roles and responsibilities to manage filtering and monitoring systems: the SLT, DSL and IT team will regularly review and oversee the effectiveness of filtering and monitoring systems

b) reviews filtering and monitoring systems at least annually to ensure compliance with national standards;

c) blocks harmful and inappropriate content without unreasonably impacting teaching and learning; and

d) has effective monitoring strategies in place that meet their safeguarding needs.

e) implements cyber security measures including multi-factor authentication (MFA), secure data storage, and regular audits of user access logs to protect sensitive data.

8.3 The Academy manages access to content across its systems for all users, including guest accounts. Logs / alerts are regularly reviewed and acted upon.

8.4 The Academy has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different abilities / ages / stages and different groups of users: staff/learners, etc.). Younger learners use child friendly / age-appropriate search engines e.g. SWGfL Swiggle.

8.5 Access to content through non-browser services e.g. apps and other mobile technologies is managed in ways that are consistent with this policy.

8.6 The Academy has monitoring systems in place to protect the Academy, systems and users. It monitors all network use across all its devices and services. Logs / alerts are regularly reviewed and acted upon.

8.7 The Academy uses a number of monitoring strategies to minimise safeguarding risks on internet connected devices, including:

a) physical monitoring by staff watching screens of users;

b) live supervision by staff on a console with device management software;

c) network monitoring using log files of internet traffic and web access; and

d) individual device monitoring through software or third-party services.

9 Access to the Academy's technology

9.1 The Academy provides internet, intranet access and an email system to pupils and staff as well as other technology. Pupils and staff must comply with the respective acceptable use policy when using Academy technology. All such use is monitored by the ICT team. Staff and students will follow updated security protocols including:

- a) Cyber security training will be mandatory for all staff to prevent the risk of cyber threats

  b) Cloud solutions used by the Academy must meet DfE standards for security, data protection and accountability

  c) Regular risk assessments will be conducted to identify potential vulnerabilities in digital infrastructure.

9.2 Pupils and staff require individual usernames and passwords to access the Academy's internet, intranet and email systems which must not be disclosed to any other person. Any pupil or member of staff who has a problem with their usernames or passwords must report it to the ICT team immediately.

9.3 No laptop or other mobile electronic device may be connected to the Academy network without the consent of the School Business Manager or

ICT Director. The use of any device connected to the Academy's network will be logged and monitored by the ICT team. See also 8.6 and the Academy's Acceptable Use policy (including remote working and bring your own device to work).

9.4 The Academy has a separate wireless network connection available for use by visitors to the Academy. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the wireless network. Use of this service will be logged and monitored by the ICT team.

9.5 Inappropriate material

9.5.1 The Academy recognises the importance of ensuring that all pupils are safeguarded from potentially harmful and inappropriate material online.

9.5.2 Online safety is a key element of many school policies and procedures and an important part of the role and responsibilities of the DSL. The term "online safety" encapsulates a wide range of ever evolving issues but these can be classified into four main areas of risk:

a) Content: being exposed to illegal, inappropriate or harmful content (e.g. pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism);

b) Contact: being subjected to harmful online interaction with other users (e.g. peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom and/or exploit them for sexual, criminal, financial or other purposes);

c) Conduct: online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending and receiving explicit images (such as the consensual and non-consensual sharing of nudes and semi-nudes and / or pornography), sharing other explicit images and online bullying; and

d) Commerce: risks such as online gambling, inappropriate advertising, phishing and / or financial scams.

9.6 Use of mobile electronic devices and smart technology

9.6.1 The Academy does all that it reasonably can to limit children's exposure to the risks identified above through the use of the Academy's IT system.

9.6.2 The Academy has appropriate filtering and monitoring systems in place to protect pupils using the internet (including email text messaging and social media sites) when connected to the Academy's network and their effectiveness is regularly reviewed.

9.6.3 Mobile devices and smart technology equipped with a mobile data subscription can, however, provide pupils with unlimited and unrestricted access to the internet. The Academy is alert to the risks that such access presents, including the risk of pupils sexually harassing, bullying or controlling their peers using their mobile or other smart technology; or sharing indecent images consensually or non-consensually(often via large group chats); or viewing and / or sharing pornography and other harmful content, and has mechanisms in place to manage such risks.

9.6.4 [*Include details, or cross-refer to separate written protocols, setting out how the Academy manages the above risks. Schools and colleges should carefully consider how this is managed on their premises and reflect in their mobile and smart technology policy and their safeguarding and child protection policy*[1]].

9.6.5 In certain circumstances, a pupil may be given permission to use their own mobile device or other smart technology to connect to the internet using the Academy's network. Permission to do so must be sought and given in advance.

9.6.6 The Academy rules about the use of mobile electronic devices or other smart technology, including access to open / non-Academy networks, are set out in the acceptable use policy for pupils.

9.6.7 The use of mobile electronic devices by staff is covered in Code of Conduct, Acceptable use policy and Social media policy, Data protection policy. Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for Academy purposes except in an emergency.

9.6.8 The Academy's policies apply to the use of technology by staff and pupils whether on or off Academy premises and appropriate action will be taken where such use affects the welfare of other pupils or any member of the Academy community or where the culture or reputation of the Academy is put at risk.

10 Procedures for dealing with incidents of misuse

10.1 Staff, pupils and Parents are required to report incidents of misuse or suspected misuse to the Academy in accordance with this policy and the Academy's safeguarding and disciplinary policies and procedures. Misuse of technology will be treated as a behavioural as well as a safeguarding issue:

- Cyberbullying, harassment or inappropriate content sharing will be addressed under both the Behaviour Policy and the Safeguarding policy with appropriate sanctions as required
- Support for victims of cyberbullying will include mental health resources, parental engagement and reporting mechanisms.

[1] [Drafting note: KCSIE requires schools and colleges to carefully consider how this is managed on their premises and to reflect this in their mobile and smart technology policy and their child protection policy.]

10.2 The Academy recognises the importance of acknowledging, understanding and not downplaying behaviours which may be related to abuse and has appropriate systems in place to ensure that pupils can report any incidents of abuse, whether or not they include an online element, confidently and safely in the knowledge that their concerns will be treated seriously. Staff should however be careful not to promise that a concern will be dealt with confidentially at an early stage as information may need to be shared further (e.g. with the DSL) to discuss next steps.

10.3 Misuse by pupils

10.3.1 Anyone who has any concern about the misuse of technology by pupils should report it immediately to the appropriate member of staff (referred to in the table below) so that it can be dealt with in accordance with the Academy's behaviour policies, including the anti-bullying policy where there is an allegation of cyberbullying.

Type of misuses	Relevant policy	Reporting channel
Bullying	**Anti-bullying**	**[• Designated member of staff / online safety lead]** **Note any incidents which give rise to safeguarding concerns must be referred on to the DSL**
Sharing nudes and semi-nude images (sexting / youth produced sexual imagery)	**Safeguarding and child protection policy and procedures** **[Sexual harassment / child-on-child abuse policy (if separate)]**	**[• Form Tutor / designated member of staff]** **Who should then refer to the DSL who has overall responsibility for online safety matters**
Sexual violence and sexual harassment (whether during or outside of school)	**Safeguarding and child protection policy and procedures** **[Sexual harassment / child-on-child abuse policy (if separate)]**	**[• The DSL who has overall responsibility for online safety matters]**
Harassment	**Safeguarding and child protection policy and procedures**	**[• Form Tutor / designated member of staff]** **Who should then refer to the DSL who has**

	[Sexual harassment / child-on-child abuse policy (if separate)]	**overall responsibility for online safety matters.**
Upskirting	**Safeguarding and child protection policy and procedures** **[Sexual harassment / child-on-child abuse policy (if separate)]**	**[• Form Tutor / designated member of staff]** **Who should then refer to the DSL who has overall responsibility for online safety matters**
Radicalisation	**Safeguarding and child protection policy and procedures** **[Prevent risk assessment / policy (if separate)]**	**[• Form Tutor / designated member of staff]** **Who should then refer to the DSL who has overall responsibility for online safety matters**
Other breach of acceptable use policy	**See relevant policy referred to in acceptable use policy**	**[• Form Tutor / designated member of staff]** **Who should then refer to the DSL who has overall responsibility for online safety matters**

10.3.2 Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the Academy's child protection procedures (see the CST Safeguarding and child protection policy and procedures).

10.4 Misuse by staff

10.4.1 If anyone has a safeguarding-related concern relating to staff misuse of technology, they must report it immediately in accordance with the Academy's policy on raising concerns and allegations, which is set out in the Safeguarding and child protection policy and procedures.

10.4.2 Anyone who has any other concern about the misuse of technology by staff should report their concerns as set out below:

a) Staff should speak to their [• Head of Department / Line Manager]in accordance with the staff whistleblowing policy; and

b) Anyone else should speak to the Headteacher.

10.5 Misuse by any user

10.5.1 Anyone who has any concern about the misuse of technology by any other user should report it immediately to the DSL or the ICT Director.

10.5.2 The Academy reserves the right to withdraw access to the Academy's network by any user at any time and to report suspected illegal activity to the police.

10.5.3 If the Academy considers that any person is vulnerable to radicalisation, the Academy will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

11 Education

11.1 The teaching of online safety is integrated, aligned and considered as part of the whole-school safeguarding approach and wider staff training and curriculum planning.

11.2 The Academy ensures that children are taught how to keep themselves and others safe, including online, and the safe use of technology is therefore integral to the Academy's curriculum. Pupils are educated in an age appropriate manner about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices (see the Academy's curriculum policy). **Teaching is tailored to the specific needs and vulnerabilities of individual children, such as those who are victims of abuse, children with SEN or disabilities.**

11.3 The safe use of technology is a focus in all areas of the curriculum and teacher training, and key safety messages are reinforced as part of assemblies and tutorial / pastoral activities and teaching pupils:

11.3.1 about the risks associated with using the technology and how to protect themselves and their peers from potential risks;

11.3.2 about the importance of identifying, addressing and reporting inappropriate behaviour, whether on or offline, and the risks of downplaying such behaviour as, for example, "*banter*" or "*just boys being boys*";

11.3.3 to be critically aware of content they access online and guided to validate accuracy of information;

11.3.4 how to recognise suspicious, manipulative, dishonest, bullying or extremist behaviour;

11.3.5 the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

11.3.6 the consequences of negative online behaviour;

11.3.7 how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the Academy will deal with those who behave badly; and

11.3.8 how to respond to harmful online challenges and hoaxes.

11.4 The Academy recognises the crucial role it plays in relation to preventative education and that this is most effective in the context of a whole-school approach that prepares pupils for a life in modern Britain and creates a culture of zero tolerance for sexism, misogyny /misandry, homophobia, biphobia and sexual violence and sexual harassment.

11.5 Pupils are taught about the risks associated with all forms of abuse, including physical abuse and sexual violence and sexual harassment which may include an online element. The Academy has a zero tolerance approach to sexual violence and sexual harassment and such behaviour is never acceptable and will not be tolerated. The Academy will treat any such incidents as a breach of discipline and will deal with them under the Academy's Behaviour policy and also as a safeguarding matter under the CST Safeguarding and child protection policy and procedures.

11.6 Those parts of the curriculum which deal with the safe use of technology are reviewed on a regular basis to ensure their relevance.

11.7 The Academy's Acceptable use policy for pupils sets out the Academy rules about the use of technology including internet, email, social media and mobile electronic devices, helping pupils to protect themselves and others when using technology. Pupils are reminded of the importance of this policy on a regular basis.

11.8 The Academy recognises that effective education needs to be tailored to the specific needs and vulnerabilities of individual pupils, including those who are victims of abuse, and those with special educational needs and disabilities, and this is taken into account when devising and implementing processes and procedures to ensure the online safety of its pupils. For more details on the Academy's approach, see the CST Safeguarding and child protection policy and procedures and [· relationships education / RSE / PSHE /other curriculum policy.][2]

11.9 Technology is included in the educational programmes followed in the EYFS in the following ways:

11.9.1 children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;

11.9.2 children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and

[2] Include links as applicable

technology; and children are guided to recognise that a range of technology is used in places such as homes and schools and encouraged to select and use technology for particular purposes.

11.10 Useful online safety resources for pupils:

ii. http://www.thinkuknow.co.uk/

iii. http://www.childnet.com/young-people

iv. [*EYFS only/delete if not relevant*]https://childnet.com/resources/smartie-the-penguin]

v. [*EYFS only/delete if not relevant*]https://www.childnet.com/resources/digiduck-stories]

vi. https://www.saferinternet.org.uk/advice-centre/young-people

vii. https://mysafetynet.org.uk/

viii. https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/

ix. https://www.bbc.com/ownit

12 Training

12.1 Proprietor

11.1.1 To ensure that all Trustees are equipped with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures of the Academy are effective and that they support the delivery of a robust whole school approach to safeguarding, all Trustees receive appropriate safeguarding and child protection (including online safety) training at induction. This training is regularly updated.

12.2 Staff

12.2.1 The Academy provides training on the safe use of technology to staff so that they are aware of how to protect pupils and themselves from the risks of using technology and to deal appropriately with incidents involving the use of technology when they occur, including managing cyber security risks and data protection and understanding the role of filtering and monitoring systems in safeguarding. This includes being able to recognise the additional risks that children with SEN and disabilities (**SEND**) face online and they are confident they have the capability to support SEND children to stay safe online.

12.2.2 Induction training for new staff includes training on the Academy's online safety strategy including this policy, the staff code of conduct, staff IT acceptable use policy and social media policy. Training specifically addresses the Academy's filtering and monitoring provisions in place, how to manage them effectively, how to escalate concerns when identified and any particular staff expectations or responsibilities.

12.2.3 Staff training is regularly updated and ongoing staff development training includes (but is not limited to) training on technology safety together with specific safeguarding issues including sharing nudes and semi-nudes images and or videos, cyberbullying, radicalisation and dealing with harmful online challenges and online hoaxes. This training may be in addition to the regular safeguarding and child protection (including online safety) updates, as required at induction and at least annually thereafter.

12.2.4 Where pupils wish to report a safeguarding concern, all staff are taught to reassure victims that they are being taken seriously and that they will be supported and kept safe. Staff are aware of the importance of their role in dealing with safeguarding and wellbeing issues, including those involving the use of technology, and understand that a victim should never be given the impression that they are creating a problem by reporting abuse, including sexual violence or sexual harassment, and nor should they ever be made to feel ashamed for making a report.

12.2.5 Where safeguarding incidents involve an online element such as youth produced sexual imagery, staff will not view or forward sexual imagery reported to them and will follow the Academy's policy on sharing nudes and semi-nude images and videos as set out in the CST Safeguarding and child protection policy and Procedures] and Searching, screening and confiscation: advice for schools (DfE, September 2022). In certain cases , it may be more appropriate for staff to confiscate a pupil's devices to preserve any evidence and hand it to the police for inspection.

12.2.6 Staff are encouraged to adopt and maintain an attitude of 'it could happen here' where safeguarding is concerned, including in relation to sexual violence and sexual harassment, and to address inappropriate behaviours (even where such behaviour appears relatively innocuous) as this can be an important means of intervention to help prevent problematic, abusive and / or violent behaviour in the future

12.2.7 Staff are trained to look out for potential patterns of concerning, problematic or inappropriate behaviour and, where a pattern is identified, the Academy will decide on an appropriate course of action to take. Consideration will also be given as to whether there are wider cultural issues within the Academy that facilitated the occurrence of the inappropriate behaviour and, where appropriate, extra teaching time and / or staff training will be delivered to minimise the risk of it happening again.

12.2.8 Staff also receive data protection training on induction and at regular intervals afterwards.

12.2.9 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the Academy's overarching approach to safeguarding.

12.2.10 Useful online safety resources for staff:

1. https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals
2. http://www.childnet.com/teachers-and-professionals
3. https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
4. https://www.thinkuknow.co.uk/teachers/
5. http://educateagainsthate.com/
6. https://www.commonsense.org/education/
7. Cyberbullying: advice for head teachers and school staff (DfE, November 2014)
8. Advice on the use of social media for online radicalisation (DfE and Home Office, July 2015)
9. Sharing nudes and semi-nudes: advice for education settings working with children and young people (DfDCMS and UKCIS, December 2020)
10. Using External Expertise to Enhance Online Safety Education (**UKCIS, October 2022)**
11. Online safety in schools and colleges: questions from the governing board (UKCIS, June 2020)
12. Education for a connected world framework (UKCIS, June 2020)
13. https://www.lgfl.net/online-safety/resource-centre
14. Online Sexual Harassment: Understand, Prevent and Respond Guidance for Schools (Childnet, March 2019)
15. Myth vs Reality: PSHE toolkit (Childnet, April 2019)
16. SELMA Hack online hate toolkit (SWGFL, May 2019)
17. Teaching online safety in school: Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects **(DfE, January 2023)**
18. Harmful online challenges and online hoaxes (DfE, February 2021)
19. Professionals online safety helpline: helpline@saferinternet.org.uk, 0344 381 4772.
20. NSPCC helpline for anyone worried about a child - 0808 800 5000
21. Internet Watch Foundation - internet hotline for the public and IT professionals to report potentially criminal online content

11.2.11 The [• name] local safeguarding partners have produced guidance for Parents on radicalisation which is available here: [*insert web link*].

12.3 Parents

12.3.1 The Academy is in regular contact with parents and carers and uses its communications to reinforce the importance of ensuring that children are safe online. The Academy aims to help parents understand what systems are in place to filter and monitor their child's online use and ensures that parents are aware of what their children are being asked to do online (including what sites they will be asked to access) and who from the Academy they will be interacting with online, if anyone.

12.3.2 [*Include details as to how the Academy informs, communicates with and educates Parents in the safe use of technology. Interactive engagement with Parents with regular and relevant online safety resources and sessions being offered is considered to be best practice*]

12.3.4 Parents are encouraged to read the acceptable use policy for pupils with their child to ensure that it is fully understood.

12.3.5 Useful online safety resources for Parents

1. https://www.saferinternet.org.uk/advice-centre/parents-and-carers
2. http://www.childnet.com/parents-and-carers
3. https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
4. https://www.thinkuknow.co.uk/parents/
5. http://parentinfo.org/
6. http://parentzone.org.uk/
7. https://www.internetmatters.org/
8. https://www.commonsensemedia.org/
9. Advice for parents and carers on cyberbullying (DfE, November 2014).
10. http://www.askaboutgames.com
11. https://www.ceop.police.uk/safety-centre
12. UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use (February 2019)
13. LGfL: parents - scare or prepare
14. Thinkuknow: what to do if there's a viral scare online

13 Mobile phones

13.1 In line with DfE guidance, mobile phone usage is prohibited throughout the school day unless authorised by a member of SLT, including breaks and

lunchtimes. Any breach of the policy will be dealt with in line with the school's behaviour policy and will result in confiscation with repeated offences leading to further disciplinary action. The school will provide clear guidance to parents and carers on mobile phone policies at the start of each academic year.

14 Cybercrime

14.1 Cybercrime is criminal activity committed using computers and / or the internet. It is broadly categorised as either "cyber-enabled" (crimes that can happen off-line but are enabled at scale and at speed on-line) or "cyber dependent" (crimes that can be committed only by using a computer).

14.2 Cyber-dependent crimes include:

14.2.1 unauthorised access to computers (illegal "hacking"), for example, accessing a school's computer network to look for test paper answers or change grades awarded;

14.2.2 denial of service (**Dos** or **DDoS**) attacks or "booting", which are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and

14.2.3 making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

14.3 The Academy is aware that pupils with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

14.4 If staff have any concerns about a child in this area, they should refer the matter to the DSL immediately. The DSL should then consider referring to the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests. Cyber Choices does not currently cover "cyber-enabled" crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

15 Risk assessment

15.1 The Academy recognises that technology, and the risks and harms associated with it, evolve and change rapidly. The Academy will carry out regular, and at least annual, reviews of its approach to online safety, supported by risk assessments which consider and reflect the risks faced by their pupils.

15.2 Furthermore, where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.

15.3 The format of risk assessment may vary and may be included as part of the Academy's overall response to a welfare issue, including the use of individual pupil welfare plans (such as behaviour, healthcare and education plans, as appropriate). Regardless of the form used, the Academy's approach to promoting pupil welfare will be systematic and pupil focused.

15.4 The headteacher has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

15.5 Day to day responsibility to carry out risk assessments under this policy will be delegated to [name (s) or job roles] who have / has been properly trained in, and tasked with, carrying out the particular assessment.

16 Record keeping

16.1 All records created in accordance with this policy are managed in accordance with the Academy's policies that apply to the retention and destruction of records.

16.2 All serious incidents involving the use of technology will be logged centrally in the technology incident log maintained by the ICT Director.

16.3 The records created in accordance with this policy may contain personal data. The Academy's use of this personal data will be in accordance with data protection law. The Academy has published privacy notices on its website which explain how the Academy will use personal data.

17 Version control

Date of adoption of this policy	May 2025
Date for next review of this policy	May 2026