Sophia HIGH SCHOOL

Online Safeguarding Policy

2025 - 2026

ONLINE SAFEGUARDING POLICY

Ownership & Consultation	
Document sponsors (role)	CEO / Director of Education/Director of EYFS
Document authors (name)	Melissa McBride Vanessa Temple (From Sept 2022 Version) Jennifer Callaway (From Aug 2023 Version) Holly McKenna (from Aug 2024 version)

Version control	
Implementation date	August 2021
Reviewed and updated	September 2022
Reviewed and updated	September 2023
Reviewed and updated	August 2024
Reviewed and updated	August 2025
Next Review	August 2026

Online Safeguarding Policy

This is to be read in conjunction with the Safeguarding and Child Protection Policy and The Digital Safety Policy

The purpose of this policy is to:

1. Provide specific guidance for staff delivering online education at Sophia High School and to our students.
2. Set out Sophia High School's approach to safeguarding students in their care. Sophia High School recognises that the success of the Policy will depend on its effective implementation. It will, therefore, ensure the effective dissemination of this Policy with the staff at Sophia High School; it will also provide appropriate training to the staff when necessary.

1. Introduction

Sophia High School is committed to ensuring a safe and supportive environment exists for all staff and students engaging in online education provision and engagement activities.

This document is designed to provide Sophia High School staff working with students online with guidance and a set of procedures to follow to ensure that they adhere to the School's policy on the Safeguarding of Children. This document was written with specific reference to online activities including, but not limited to, interaction on online platforms, instant messaging/chat, live videos/webinars and mentoring.

Safeguarding concerns in the online education environment can take many forms including, but not limited to, bullying and cyber bullying, peer on peer abuse, youth produced sexual imagery, child sexual exploitation/trafficking, domestic abuse, emotional abuse, grooming, neglect, children missing in education, online abuse, physical abuse, sexual abuse. Abuse could be by adults, or by other children/young people.

This policy applies to all staff involved in the delivery and supervision of online work and should be read alongside the school's wider Safeguarding policies and practice. This includes school staff members, as well as temporary teachers/tutors/guests that may run workshops from time to time.

<u>We believe that:</u>

- Children and young people should never experience abuse of any kind.
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.
- Children should understand how to keep themselves safe when learning online.

We recognise that:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges.
- We have a duty to ensure that all children, young people, and adults involved in our organisation are protected from potential harm online.
- We have a responsibility to help keep children and young people safe online, whether or not they are using our Google Classroom.
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation, have the right to equal protection from all types of harm or abuse.
- Working in partnership with children, young people, their parents or guardians, and agents is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

1.1 Online safety

It is essential that children are safeguarded from potentially harmful and inappropriate online material. Our School's effective whole school approach to online safety empowers our staff to protect and educate students and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

Technology

Technology often provides the platform that may facilitate harm. All staff should be aware of the unique risks associated with online safety, and that technology is a significant component in many safeguarding and wellbeing issues. The DSL is responsible for overseeing online safety in schools and should raise awareness in the staff group accordingly, including but not limited to, cyber-bullying, child sexual exploitation, radicalisation and sexual predation.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

Content:

- being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact:

- being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct:

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

Commerce

- risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

At Sophia High, we ensure online safety is a running and interrelated theme whilst updating and implementing policies and procedures. We consider how online safety is reflected in our unique online learning environment as required in all relevant policies, consider online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the Designated Safeguarding Lead (DSL) and any parental engagement.

As part of this process, the school has appropriate filters and monitoring systems in place and regularly reviews their effectiveness. Whilst it is essential that schools ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Our Online Safeguarding Policy covers in detail how we approach remote learning in our online learning environment.

1.2 Remote learning

Where children are being asked to learn online at home the Department for Education has provided advice to support schools and colleges do so safely: safeguarding in schools colleges and other providers and safeguarding and remote education.

The NSPCC and PSHE Association also provide helpful advice:

- NSPCC Learning - Undertaking remote teaching safely during school closures
- PSHE - PSHE Association coronavirus hub

1.3 Filters and monitoring

SHS meets the Cyber Security Standards and has been issued a certificate. Staff have been trained in Cyber security and have been issued certificates. The school follows the recently published DFE Publication of Filtering and Monitoring Standards and Guidance.

Whilst considering our responsibility to safeguard and promote the welfare of children and provide our students with a safe environment in which to learn, our education team and proprietors are doing all that we reasonably can to limit children's exposure to risks outlined in our Remote Learning Risk Assessment from the school's Digital Education Platform.

As part of this process, we ensure our school has appropriate cyber security and monitoring systems in place through Google for Education. We consider the age range of our children, the number of children, how often they access the system and the proportionality of costs vs risks.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and are informed in part, by the risk assessment required by the Prevent Duty. The UK Safer Internet Centre has published guidance as to what “appropriate” filtering and monitoring might look like:
UK Safer Internet Centre: appropriate filtering and monitoring.

The Prevent duty:
https://assets.publishing.service.gov.uk/media/65e5a5bd3f69457ff1035fe2/14.258_HO_Prevent+Duty+Guidance_v5d_Final_Web_1_.pdf

Sophia High School is committed to providing a safe, secure, and effective online learning environment for all our students. As a British online school utilising Google Workspace for Education as our digital learning platform, we adhere to the Department for Education's (DfE) guidelines on filtering and monitoring, as outlined in the "Keeping Children Safe in Education" (KCSIE) policy.

Use of VPN to access the SHS platform, including live and recorded lessons:
To ensure the safety and security of our students and staff, and to maintain the integrity of our online learning environment, we strictly prohibit the use of Virtual Private Networks (VPNs) when accessing school-owned email accounts and our online learning platform.

The use of VPNs poses significant risks to our unique remote learning environment, including:

- Circumventing school and google workspace web filters and content control measures, potentially exposing students to harmful or inappropriate material.
- Concealing user activity, making it difficult for the school to monitor and detect potential safeguarding risks or unauthorised access.
- Enabling unregulated direct communication from anywhere, which may lead to student vulnerabilities and compromise the school's ability to fulfil its duty of care.
- Increasing the risk of ransomware attacks and other cyber threats, which can jeopardise the security and integrity of the school's network and student data.
- Compromising data security as VPNs can create additional entry points into the school's network, potentially compromising the security of sensitive student data and intellectual property
- Interfering with google workspace performance: The use of VPNs can strain the school's google workspace network resources and slow down internet speeds, negatively impacting the quality of the online learning experience for all students.

As part of our commitment to meeting the DfE's filtering and monitoring standards, Sophia High School employs a range of strategies to minimise safeguarding risks on internet-connected devices, including:

- Physical monitoring by staff watching user screens in online lessons
- Live supervision by staff using device management software in lessons
- Network monitoring using log files of internet traffic and web access
- Annual review of access control, security and online safeguarding or more frequently if risks

are identified.

Our filtering systems are designed to identify device names or IDs, IP addresses, and, where possible, individual users, along with the time and date of attempted access and any blocked search terms or content.

The senior leadership team is responsible for procuring, documenting, reviewing, and overseeing these systems to ensure their effectiveness in meeting our statutory requirements under KCSIE and the Prevent Duty.

We recognise that effective filtering and monitoring should not unreasonably impact teaching and learning or school administration, nor should it restrict students from learning how to assess and manage risk themselves.

As such, we conduct regular reviews of our systems, at minimum annually, or when a safeguarding risk is identified, there is a change in working practise, or new technology is introduced.

By prohibiting the use of VPNs, we aim to maintain a transparent, secure, and accountable online learning environment that allows us to effectively monitor and mitigate potential risks. We appreciate the cooperation of our students and their families in adhering to this policy, as it is essential to ensuring the safety and well-being of our entire school community.

Parents and guardians are required to acknowledge and agree to this VPN prohibition as part of the terms and conditions for enrolling their child at Sophia High School.

Any violation of this policy may result in disciplinary action, up to and including restriction of access to the online learning platform and school email accounts and/or termination of the student's enrolment.

1.4 Online Safety & Safeguarding at Sophia High School

The school will use parental communications to reinforce the importance of children being safe online. Parents may be supported to understand what systems the school uses to filter and monitor online use. The school will update parents regularly about what their children are being asked to do online in school, including the sites they will be asked to access, and with whom they may be interacting online.

Many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school, sexually harass their peers via their mobile and smart technology, share indecent images: consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content.

Schools will always work with parents to support them to address their child’s online activity as needed. All staff should also be familiar with the school’s Acceptable Use & Digital Safety Policy, which sets out the school’s approach to online safety in further detail.

Technology, and risks and harms related to it evolve and change rapidly. The school will carry out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face.

We will seek to keep children and young people safe by:

- Providing an especially safe online platform for the delivery of our online curriculum through a partnership with Google for Education.
- Google Classroom is secure and accessible only by enrolled pupils, their parents and school staff. All online students pledge to uphold the acceptable use policy and receive instruction in good digital citizenship and Internet safety by signing the Digital Safety Forms/Agreements found in the Digital Safety Policy **(Appendix A)**
- All Sophia High School staff are carefully screened and specially trained to ensure a positive school environment for everyone.
- Ensuring that appropriate cyber security controls and measures are in place in order to reduce the risk of cyber-attacks which may include **phishing** emails, **malware** from bogus websites and downloads, **ransomware** attacks and **Denial of Service attacks.**

In our online school we:

- Provide clear and specific directions to staff on how to behave online through our Code of Conduct for Staff and Volunteers including Acceptable Use Policy.
- Support and encourage the young people studying with us to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others through etiquette and beyond into Metaverse Etiquette.
- Ensure all students sign an Agreement from the Code of Conduct for Staff and Volunteers including Acceptable Use Policy. All online students pledge to uphold the Agreement and receive instruction in good digital citizenship and Internet safety), and Staying Safe Online Guidelines are shared in the Health and Safety Policy.
- Support and encourage parents, guardians, and agents to do what they can to keep children safe online by offering guidance, workshops and personal support for adults supporting learners.
- Develop clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person.
- Regularly review and update the security of our information systems.
- Ensure that usernames, logins, email accounts and passwords are used effectively.
- Ensure personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate.
- Ensure that images of children and young people are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
- Provide supervision, support and training for staff and any individual involved with Sophia High's online activities regarding online safety.
- Examine and risk assess any social media platforms and new technologies before they are used within the school.

Staff members with specific safeguarding responsibilities:

DSL: Kelly Cox kelly.cox@sophiahigh.school

DDSL: Nicole Pelletier nicole.pelletier@sophiahigh.school
DDSL (E-safety) tyler.wilson@sophiahigh.school

1.5 Disclosure

All staff should understand that even if there are no reports in their school it does not mean it is not happening, it may be the case that it is just not being reported. All members of staff (including non-teaching staff) should be aware of how to recognise and refer onwards any disclosure of incidents involving the sharing of nudes/semi-nude imagery/videos. This will be covered within staff training. Disclosure can happen in a variety of ways. The child affected may inform a class teacher, the Child Protection and Wellbeing Coordinator in school, or any member of the school staff. They may report through an existing reporting structure, or a friend or parent may inform someone in school or a colleague or inform the Police directly.

Any direct disclosure by a child should be taken very seriously. A child who discloses they are the subject of sexual imagery is likely to be embarrassed and worried about the consequences. It is likely that disclosure in school is a last resort, and they may have already tried to resolve the issue themselves.

If there is a evidence of online abuse, suspicion of abuse, or disclosure (direct or indirect), we will respond to it by:

- Referral to the DSL as soon as possible
- The DSL should hold an initial review meeting with appropriate school staff.
- There should be interviews with the children involved (if appropriate, seek advice).
- Parents of each child should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the child at greater risk of harm and jeopardise any police/social care investigation; and
- At any point in the process, if there is a concern that a child has been harmed or is at risk of harm, a referral should be made to Social Services and/or the Police immediately.
- Having clear and robust safeguarding procedures in place for responding to abuse (including Child on Child abuse in the Child on Child Abuse Policy.)
- Providing support and training for all staff on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.
- Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole, into account.
- Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

1.6 Metaverse Education

Students at Sophia High School use ground breaking Metaverse Education to support a range of curriculum areas, and also as a stand-alone curriculum to develop skills necessary for their future. The spaces that they enter are created by the SHS IT Department, and as such are private and only those with an authorised SHS email account can enter. This is a private space, much like a private classroom.

On occasion, the children may enter a public space, such as an environment on Somnium Space, and these times must be considered an External Educational Visit. A full Risk Assessment must be completed to ensure that all risks related to the environment they are entering are identified and minimised. As with all additional activities, parents will be informed of all Metaverse activities prior to their child entering the space, and any objections will be adhered to.

The guiding body of Metaverse Education is the Metaverse Education Council. Their policies and advice will be adhered to when considering all Metaverse Education experiences.
Students at Sophia High have helped shape our internal framework, "Metiquette" which will form the basis for their work within the Metaverse.

2. Scope of this Policy

This policy specifically relates to online outreach and engagement activities. This policy should be read alongside Sophia High School's Safeguarding Policy.

Legal framework:

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- online abuse https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
- bullying https://learning.nspcc.org.uk/child-abuse-and-neglect/bullying
- child protection https://learning.nspcc.org.uk/child-protection-system

3. Areas of risk

3.1 Risk Assessment

Some key risks in online activities are highlighted below. For all new activities planned, a risk assessment should be undertaken which should be approved by the CEO. This risk assessment should be shared with all members of staff involved in the online activity. **(Appendix B Blank Risk Assessment Form)**

3.2 IT Safety and Data Protection (additional requirements White Paper 2019) The below considerations are highlighted in line with the IT safety and data protection White Paper 2019.

3.2.1 A Privacy notice is provided on the school website and is easily accessible and provided in language that the participants can understand and are thus fairly informed.

3.2.2 Data protection best practice for any data gathered and stored should be considered in advance of the activity. Data protection should be considered at all stages of design ensuring the approach mitigates the risk to individual participants' information.

3.2.3 The appropriateness of the platform and how they store, process and use personal data should be considered in deciding on an appropriate platform for the delivery of any online lesson/activity.

3.2.4 For assistance in compliance with Data Protection Regulations, please contact the Data Protection Officer, Fernando Darcie: fernando.darcie@sophiahigh.school

3.3 Social Media

3.3.1 Staff must not engage or communicate with children or children's families via personal or non-school-authorised accounts – all communications should come from an official Sophia High School email account.

3.3.2 For all online activities, consent should be sought from parents/carers and the child/young person before posting any identifiable information and/or images of children and young people on social media.

3.3.3 Concerns about social media content or posts involving children and young people such as cyberbullying, self-harm, abuse or exploitations should be raised with the designated safeguarding officer in line with the process in the overarching safeguarding policy.

3.3.4 Staff and students working on online educational provision should abide by the general principles of the Code of Conduct for Staff and Volunteers including Acceptable Use Policy, Behaviour Policy, Exclusions Policy, and other relevant Sophia High School staff policies.

3.3.5 Staff and students working in our online education environment should not use social media in a way which would breach other school policies, including the Safeguarding Policy.

Ofcom produces an annual report regarding CYA and internet use. This is a valuable document for schools and parents to use as a starting point for discussions about safeguarding for the various platforms, and to raise awareness of the dangers of unregulated internet use.

3.4 Online Learning and Real Time Interactive Lessons

The measures below are as much about protecting Sophia High School staff, as they are about supporting the students engaging in these lessons/activities.

At Sophia High School, we provide a full-time education following the UK National Curriculum and International Primary Curriculum/Middle Years Curriculum through a blended learning programme which combines live interactive lessons with independent home learning.

Lessons are live streamed using our secure and password protected Google Classroom platform and teachers have full control over interactive learning tools including the recording of each lesson for safeguarding purposes. Throughout our programme, parents and students are taught how to use online learning tools safely and our programme is structured to build a sense of community/belonging amongst our student groups.

We have partnered with Google for Education, as this platform offers the world's most advanced security infrastructures in order to protect the privacy of our users. This built-in security automatically

detects and prevents online threats, so that sensitive student and school information is safe.

The school's online platform, powered by Google for Education, is secure and accessible only by enrolled pupils, their parents and school staff. Google is committed to building products that help protect student and teacher privacy and provide best-in-class security for our online school.

Google Workspace for Education and Chromebooks support compliance with rigorous standards including:

- US FERPA (Family Educational Rights and Privacy Act)
- The Software & Information Industry Association
- COPPA (Children's Online Privacy Protection Act of 1998)
- Student Privacy Pledge introduced by the Future of Privacy Forum (FPF)
- ISO/IEC 27018:2014 (Data standards)

Four things to know about Google for Education

Google takes security seriously, with industry-leading safeguards and privacy policies that put the school in control of their data.

Here's how you know that students and educators are protected when using Google for Education.

1. Google keeps your data secure. Schools own their data – it's Google's responsibility to keep it secure. Google builds and operates their own secure servers and platform services, and they make it easy for administrators to monitor and manage data security.
2. There are no ads in Google Workspace for Education core services. Students' personal information won't be used to create ad profiles for targeting.
3. Google supports compliance with industry regulations, best practices and security requirements. Independent organisations have audited Google services, ensuring their data protection practices meet demanding standards.
4. We have clear information about Google's privacy and security policies. Google is committed to transparency about their data collection policies and practices. The Google Workspace for Education Privacy Notice and Google Workspace Agreement explain their contractual obligations to protect your data.

Full information about Privacy & Security with Google for Education can be found at https://edu.google.com/intl/ALL_ae/our-values/privacy-security/

3.4.1 Where live streaming is deemed the Sophia High School has chosen *Google Classroom* as the best platform for delivery of lessons/activities. A risk assessment has been carried out by the Senior Leadership Team and is shared with all the teachers.

3.4.2 Any online activities should only be delivered via online platforms approved for use by Sophia High School.

3.4.3 Access to the individual platform should only be enabled for the intended participants and is controlled by the Administrative Team.

3.4.4 The platform enables the presenter to control microphones/cameras for participants.

3.4.5 Personal accounts for platforms are not to be used to engage with young people, all activities are organised through Google Classrooms and the school domain Google email address.

3.4.6 Personal information (including names, contact details and email addresses) is only accessible to those with approved permissions and should not be publicly viewable.

3.4.7 Staff must never give out personal details to participants such as personal email address, personal phone number or social media accounts.

3.4.8 Staff facilitating activities and monitoring any enabled chat should be able to remove people from the platform if necessary, according to Behaviour and Exclusion Policies.

3.4.9 For all live activities, staff members record sessions and have all undergone the full Safer Recruitment in Education checks. The school admin team is able to monitor messages sent on the chat platform and has access to all recorded lessons, which are reviewed. Live lesson recordings are posted daily to individual year group Google Classrooms for access by students and families with access to that Classroom so that learning is visible.

3.4.10 During a live session, staff or students organising it should:

- Ensure that the session is taking place in a neutral area where nothing personal can be seen and there is nothing inappropriate in the background.
- Monitor interactions (verbal and in live chats) to check it is appropriate and relevant, and to deal with any sudden changes or upsetting developments.

3.4.11 If a staff member leaves the session for any reason or has issues accessing the Google Meet (e.g.: connection issues), they should get in contact with the Senior Leadership Team as soon as possible (by phone if necessary) and attempt to re-join the session if possible. If it is not possible to have a staff member present, then the event should be ended as soon as reasonably possible and this should be communicated to all participants.

3.4.12 At the start, the main speaker should remind participants how to keep themselves safe (as outlined above) in addition to reminding them of the ground rules. This is also a good time to restate any pre-shared privacy notice to participants and particularly important if participants can override any central setting and share their own video unless asked by the teacher.

3.4.13 If staff share their screens at any point, they must ensure that there is nothing inappropriate on the screens/internet pages/browser history.

3.4.14 Challenging behaviour or inappropriate comments should be dealt with immediately, which may involve muting or removing the offender from the platform in line with the school Behaviour and Exclusion Policies.

3.4.15 You should also ensure that the participants:

- Do not share private information about themselves.
- Do not respond to contact requests from people they do not know.
- Understand who they should contact if they hear or see anything upsetting or

inappropriate.

3.4.16 For any interactive live streaming, consent is sought and recorded from parents/guardians of any under-18 participants.

3.4.17 A signed Code of Conduct for Staff and Volunteers including Acceptable Use Policy should be received from all participants which should include the consequences in the case of inappropriate behaviour.

3.4.18 At the start of a session participants should be reminded of this Code of Conduct, not to take photographs of the screens or share any images, and how they can report any concerns.

3.4.19 If a safeguarding disclosure is made by a participant, the School's Safeguarding Policy should be followed.

3.4.20 For academic support or assessment purposes, members of staff may be in a Breakout Room with an individual student, and no record function is possible as the main session is being recorded. On these occasions, the teacher and individual child will remain in the Google Classroom where the work can be recorded, and the group and additional teacher will work in the unrecorded Breakout Room. All risks must be considered and so a Risk Assessment has been completed to show how risks in this situation can be minimised.

Indicators

Signs of grooming and/or online abuse

A child may be experiencing abuse online if they:

- Spend lots, much more, or much less time online, texting, gaming or using social media.
- Are withdrawn, upset or outraged after using the internet or texting.
- Are secretive about who they're talking to and what they're doing online or on their mobile phone; and/or
- Have lots of new phone numbers, texts or e-mail addresses on their mobile phone, laptop or tablet.
- Have more than one phone.

Sharing of nudes/semi nudes imagery/videos (previously referred to as Youth Produced Sexual Imagery and/or 'sexting')

Whilst many professionals refer to the issue as 'sexting', there is no clear definition of 'sexting'. According to research, many professionals consider sexting to be 'sending or posting sexually suggestive images, including nude or semi nude photographs, via mobiles or over the internet.'

This policy only covers the sharing of sexual imagery by children. Possessing, creating, sharing and distributing sexual photos and videos of under-18s is illegal, and therefore causes the greatest complexity for schools (amongst other agencies) when responding. It also presents a range of risks which need careful management.

What types of incidents are covered by this policy?

- A child creates and shares sexual imagery of themselves with a peer (also under the age of 18).
- A child shares sexual imagery created by another child with a peer (also under the age of 18) or an adult.
- A child is in possession of sexual imagery created by another child.
- The sharing of sexual imagery of children by adults as this constitutes child sexual abuse and schools should always inform the Police. Images of this kind should not be deleted from a child or adult's phone.
- Children sharing adult pornography or exchanging sexual texts which do not contain imagery as such incidents should be responded to with reference to the school's Online Safety Policy, and in line with the school's Safeguarding Policy Safeguarding and Child Protection Policy and Procedure
- Sexual imagery downloaded from the internet by a child
- Sexual imagery downloaded from the internet by a child and shared with a peer (also under the age of 18) or an adult.

Contextual Safeguarding

Contextual Safeguarding is an approach to understanding, and responding to, young people's experiences of significant harm beyond their families. It recognises that the different relationships that young people form in their neighbourhoods, schools and online can feature violence and abuse. Parents and carers have little influence over these contexts, and young people's experiences of extra-familial abuse can undermine parent-child relationships.

Staff should consider the importance of understanding intra familial harms and any necessary support for siblings following incidents of Peer-on-Peer abuse, including sexual harassment and/or violence.

The contextual safeguarding approach says that children's social care practitioners, child protection systems and wider safeguarding partnerships need to engage with individuals and sectors who do have influence over/within extra-familial contexts, and recognise that assessment of, and intervention with, these spaces are a critical part of safeguarding practices.

Contextual Safeguarding, therefore, expands the objectives of child protection systems in recognition that young people are susceptible to abuse beyond their front doors. This also includes the risk of abuse occurring in or outside of school.

4. Disclosure and Barring Service Checks (DBS)

DBS checks are required for all staff involved in online delivery; the requirements for this are outlined in our School's Safer Recruitment Policy.

Records of pre-employment checks and subsequent training are held by the CEO and Head of Admissions in the School's Single Central Register.

5. Key contact details

For questions, to discuss this policy further or raise a concern, please contact Designated Safeguarding Lead (DSL), Kelly Cox, by emailing kelly.cox@sophiahigh.school

6. Links to other Sophia High School Policies and Procedures

Related documentation	
Related documentation	Code of Conduct for Staff and Volunteers including Acceptable Use Policy. Health and Safety Policy Safer Recruitment Policy Sophia High School's Safeguarding Policy Child on Child Abuse Policy Youth Produced Sexual Imagery Policy Behaviour Policy Anti Bullying Policy
Document Author (s)	Melissa McBride David McCarthy Vanessa Temple Jennifer Callaway Holly McKenna Rosanna Sparks
Audience	Staff, Students, Prospective Students and their Families
Policy Location	SIP, Google Classroom, External Website
Implementation date	6th August 2021
Reviewed	September 2022 April 2023 April 2024 April 2025 / August 2025
Next Review date	August 2026

Equality Analysis: The policy has been developed with due regard to the school's equality duty.

Appendix A

Annex 1 Digital Safety Agreement for Pupils in Years 1-2

These are our rules for using the internet safely at school:

- We use the internet safely to help us learn.
- We learn how to use the internet.
- If we see anything on the internet or receive a message that is unpleasant, we must tell an adult.
- We learn to keep our password a secret.
- We know who and when to ask for help.
- If we see something on a computer that we do not like or makes us feel uncomfortable we know what to do.
- We know that it is important to follow the rules.
- We aim to look after each other by using the internet safely.
- We will consider the implications for misusing the internet and technology, for example, posting inappropriate materials to websites; deleting work from digital notebooks, shared folders and drives.

Name:_____Year group:_____

I understand the Digital Safety Agreement for using the internet, email and online tools safely and responsibly. I am aware that the adults working with me at school will help me to check that I am using the computers appropriately.

Pupil signature:_____Date: _____

Annex 2 – Digital Safety Agreement for Pupils in Years 3-6

These are our rules for using the internet safely and responsibly at school:

- We use the internet to help us learn, and we will learn how to use the internet safely and responsibly.
- We send emails and messages that are polite.
- Approval from an adult may be needed before we email, chat to, or video-conference anyone at school.
- We never give out passwords or personal information (like our last name, address or phone number).
- We never post photographs or video clips without a teacher's permission and never include names with photographs.
- If we need help we know who and when to ask.
- If we see anything on the internet or in an email or other electronic message that makes us uncomfortable or appears unpleasant, we inform an adult.
- I accept that the school monitors my use of the internet at school and my school email account.
- If we receive a message sent by someone we do not know, we inform an adult.
- We aim to look after each other by using our safe internet in a responsible way.
- We agree not to send hurtful words, images or messages outside of school on the internet or mobile devices about anyone in our school community.
- We will consider the implications for misusing the internet and technology, for example, posting inappropriate materials to websites; deleting work from digital notebooks, shared folders and drives.
- I am aware of the Metaverse etiquette that my teacher has shared with me.

Name:_____Year group:_____

I understand the Digital Safety Agreement for using the internet, email and online tools safely and responsibly. I am aware that the adults working with me at school will help me to check that I am using the computers appropriately.

Pupil signature:_____Date: _____

Annex 3 – Digital Safety Agreement for Pupils in Years 7+

I am encouraged to use and be aware of the safety rules and procedures which regulate my use of the ICT resources, including the internet. Access to the school's network and the internet enables me to find resources, to communicate, and to help my research for the completion of school work.

- I accept that these facilities are to be used for educational purposes only and in an appropriate manner. I take responsibility for my actions and know that any breach of the rules will be considered a serious disciplinary matter.
- I will make targeted use of the internet to support my studies.
- I accept that the school monitors my use of the internet at school.
- I will not access, create or display any material (images, sounds, text, and video) which is likely to cause offence, inconvenience or anxiety to anyone.
- I will fully follow our teachers' instructions over the use of IT and the internet.
- I do not assume that information published on the Web or written in an email is accurate. I keep my username and password confidential.
- I am careful about what I write on a computer. I check my work before I print or send it.
- I do not use bad language. I do not write racist, sexist, abusive, homophobic or aggressive words. I do not write things that could upset or offend others.
- I understand that sending malicious messages outside of school can become a matter whereby the school will set sanctions or involve outside agencies such as the police.
- I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
- I do not make available online personal information about myself or anyone else, such as an address, telephone number and private details, in an email or on a website.
- I do not respond to offensive, abusive or rude messages. I let a teacher know immediately if I am sent anything I do not feel comfortable with.
- At school I do not go to sites or download any materials which are in bad taste, offensive, violent or pornographic.
- If I quote from a text I will always attribute my sources and acknowledge use of anyone else's ideas, images or data by citing the author, using quotation marks, and compiling a bibliography as required.
- I always respect the privacy of other users' data.
- I will check my school emails through the Learning Management System regularly to enable me to work and learn effectively.
- I will follow the school rules on academic honesty and not practise plagiarism.
- I know that if I am worried about something related to technology outside of school I can ask for advice or help from my teachers.
- We will consider the implications for misusing the internet and technology, for example, posting inappropriate materials to websites; deleting work from digital notebooks, shared folders and drives.
- I am aware of the Metaverse etiquette that my teacher has shared with me.

Name:_____Year group:_____

I understand the contents of the school's Digital Safety Agreement and the rules for using the internet, email and online tools safely and responsibly. I am aware that the adults working with me at school will help me to check that I am using the computers appropriately.

Pupil signature:_____Date: _____

Appendix B.

Remote Learning Risk Assessment (Blank template)

Area/Facility	Risk Title	Risk Details	Impact	Control/Activities	Lead