ONLINE SAFETY POLICY

Date of policy review:	September 2025
Date for review:	September 2026
Lead for review:	Deputy Head Pastoral

Contents

Key Contacts

School Contacts

Name of School:

Guildhouse School London

Headteacher:

Ian Gross (igross@guildhouseschool.com)

Online safety coordinator:

Jamie Forbes (jforbes@guildhouseschool.com)

IT systems/Data manager:

Chris Little (clittle@catsglobalschools.com)

Designated safeguarding lead (DSL):

Jamie Forbes (jforbes@guildhouseschool.com)

Nominated governor:

Liz Francis (lfrancis@catsglobalschools.com)

London Borough of Camden Contacts

Child protection service manager:

Kurt Ferdinand: 020 7974 6481

Local Authority Designated Officer (LADO):

Jacqueline Fearon: 0202 7974 4556

Email: LADO@camden.gov.uk

Children's Contact Service/MASH team:

Tracey Murphy: 020 7974 1553/3317

Fax: 020 7974 3310

Prevent Co-ordinator/ Education Manager

Jane Murphy: 020 7974 1008

Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Guildhouse School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping the safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with Central IT colleagues (e.g. for filtering and monitoring), Pastoral Directors (e.g. PSHE/RSHE curriculum planning) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school entrance and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Helping school staff working with students to understand their roles and responsibilities to work safely and responsibly with technology and the online world: for the protection and benefit of the young people in their care, and for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice. For the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies (such as the Student Behaviour Policy or Anti-Bullying Policy)

Roles and responsibilities

This policy applies to all members of the Guildhouse School community who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time. A successful online safety strategy needs to be inclusive of the whole school community, including teachers, boarding staff, governors and others, and forges links with parents and the sales team. The strategy is overseen by the DSL/Headteacher and fully implemented by all staff, including operations and non-teaching staff. Guildhouse School is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to immediately report any concerns or inappropriate behaviour, to protect staff, students, families and the reputation of the school.

Headteacher's role

The Headteacher must have ultimate responsibility for online safety issues within the school including:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership (Camden) support and guidance.

- Ensure all staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures.
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles in line with the Central IT Team infrastructure.
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the DfE standards, through regular liaison with IT colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
- Liaise with the Designated Safeguarding Lead on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of students, including risk of children being radicalised.
- Ensure the school website meets statutory requirements

<u>Governors' role</u>

- Approve this policy and strategy and subsequently review its effectiveness
- Undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the online safety coordinator / DSL.
- Work with the DPO, DSL and headteacher to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum
- Ensure that there are policies and procedures in place to keep students safe online and that these are reviewed regularly.
- Liaise with IT staff and service providers to annually review school IT filtering and monitoring systems to check their effectiveness and ensure that the school leadership team are aware of what provision is in place and how to escalate any concerns.

- Governors should be subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct.

- Governors should always use business email addresses when conducting school business.

Online safety coordinator's role

The school's designated online safety coordinator (the DSL) is responsible for co-ordinating online safety policies on behalf of the school.

- The DSL should take lead responsibility for safeguarding and child protection including online safety and understanding the filtering and monitoring systems and processes in place.
- Ensure an effective whole school approach to online safety as per KCSIE.
- Ensure the school is complying with the DfE's standards on Filtering and Monitoring. As part of this, the DSL will liaise with the IT team to carry out reviews and checks on filtering and monitoring, to compile the relevant documentation and ensure that safeguarding and technology work together.
- Ensure all staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated. This includes understanding filtering and monitoring and helping them to understand their roles. All staff must read KCSIE Part 1
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.
- The log of internet related incidents and co-ordination of any investigation into breaches will be maintained and led by the DSL.
- Work closely with SLT and IT colleagues when appropriate to complete online safety audits (including technology in use in the school)
- Work with the headteacher, DPO and governors to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding and undertake Prevent awareness training.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based/
- Receive regular updates about online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance.
- Promote an awareness of and commitment to online safety throughout the school community, including communication with parents and stakeholders.
- Communicate regularly with SLT and the safeguarding governor to discuss current issues, review incident logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for students to disclose issues when off site. The DSL and other Level 3 SLT members of staff can be contacted on

Microsoft Teams outside of school hours and students can also email: concern@guildhouseschool.com

- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).
- Ensure that all staff and students have read and signed the acceptable use policy (AUP)
- Report annually to the board of governors on the implementation of the school's online safety strategy.

Director of IT's role

- Ensure the maintenance and monitoring of the school internet system including anti-virus and

filtering systems.

- Ensure that filtering and monitoring systems are robust and comply with the Department of Education Filtering and monitoring standards for schools **Meeting Digital and Technology Standards in Schools and Colleges - Filtering and Monitoring standards for schools and colleges Guidance** https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges and with **Keeping Children Safe in Education 2025** https://assets.publishing.service.gov.uk/media/68add931969253904d155860/Keeping_children_safe_in_education_from_1_September_2025.pdf
- Carry out monitoring and audits of networks and reporting breaches to the DSL
- Support any subsequent investigation into breaches and preserving any evidence

Role of School staff

All school staff have a dual role concerning their own internet use and providing guidance, support and supervision for students. Their role is:

- Adhering to the school's online safety and acceptable use policy and procedures.
- Communicating the school's online safety and acceptable use policy to students as part of their induction.
- Keeping students safe and ensuring they receive appropriate supervision and support whilst using the internet.
- Planning the use of the internet for lessons and researching online materials and resources.
- Reporting any concerns or breaches to the online safety coordinator/DSL immediately.
- Maintaining an awareness of current online safety issues and guidance (KCSIE 2025)
- Modelling safe, responsible and professional behaviours in their own use of technology at school and beyond.
- Being aware of the filtering and monitoring system in use and making the online safety coordinator/DSL aware of any students bypassing protections.
- Being responsible for the physical monitoring of students' online devices during any session/class they are working within.
- Recognising when students are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the online safety co-ordinator/DSL
- Teaching the online safety and digital literacy elements of the RSHE curriculum (Personal Tutors/Teaching staff).

- Working closely with the DSL and Pastoral Directors to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE. (Personal Tutors/Teaching staff)
- Embedding and delivering content (Personal Tutors/Teaching staff) on consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from latest trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum.
- Teaching what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online.
- Addressing online safety and appropriate behaviour in an age-appropriate way.
- Helping students to navigate the online world safely and confidently regardless of their device, platform or app and identifying where students may need extra support or pastoral intervention

Designated Safeguarding Lead

Where any online safety incident has serious implications for the child's safety or well-being, the matter should be referred to the designated safeguarding lead for the school who will decide whether or not a referral should be made to Children's Safeguarding and Family Help or the Police. In some schools, the designated safeguarding lead will be the online safety co-ordinator

Working with parents and carers

It is essential that the school involves parents and the student recruitment team in the development and implementation of online safety strategies and policies; most students will have internet access at home or their own mobile devices and might not be as closely supervised in its use as they would be at the school.

Therefore, parents and the sales team need to know about the risks so that they are able to continue online safety education at home and regulate and supervise students use as appropriate to their age and understanding.

The Headteacher, board of governors and the online safety coordinator should consider what strategies to adopt in order to ensure parents are aware of online safety issues and support them in reinforcing online safety messages at home.

Students with special educational needs and disabilities (SEND)

Students with special educational needs and disabilities (SEND) may be more vulnerable to risk from use of the internet and may need additional guidance on online safety practice as well as closer supervision.

Teaching online safety

Guildhouse School adopts a whole-school approach to online safety, with the aim of empowering students to use technology safely, responsibly, and independently.

- The Headteacher and Online Safety Coordinator oversee the design and implementation of online safety education.

- All staff contribute to promoting online safety, both in and beyond the classroom.

- The Online Safety Coordinator ensures staff are equipped with the necessary training and resources.
- Personal tutors and teachers deliver online safety education through the curriculum, especially in PSHE, and RSE.
- Staff monitor and support students' use of devices including personal devices and mobile phones in line with school policies.
- Staff should be alert to students who may be more at risk online, such as those with SEND or high digital competence but low social awareness.

Curriculum Content

Online safety is taught through a sequenced and age-appropriate PSHE/RSHE curriculum that builds knowledge, skills, and resilience. It is embedded across year groups and tailored to students' developmental stages and student needs.

Students learn to:

- Use technology safely and respectfully.
- Protect personal information.
- Seek help when concerned about online content or contact.
- Apply critical thinking to digital information and technologies.
- Become confident, responsible, and creative digital citizens.

Statutory RSE & Health Education Topics

Students are taught:

- Types and impact of bullying, including cyberbullying.
- Online rights, responsibilities, and behavioural expectations.
- Risks of sharing personal or compromising material online.
- How to report concerns and access support.
- The impact of harmful content, including pornography.
- Legal implications of sharing indecent images, including self-generated content.
- How online data is collected, shared, and used.
- Differences between online and offline worlds.
- Risks of unhealthy comparisons, online gambling, and targeted advertising.
- Recognising and reporting harmful online behaviours.

Online safety education:

- Builds on prior knowledge and is age appropriate.

- Addresses risks and promotes safe behaviours across platforms and devices.
- Is responsive to emerging issues (e.g. misinformation, deepfakes, AI risks).
- Includes reactive support where filtering and monitoring or classroom activity identifies students needing intervention.

Whole-School Integration

Online safety is not confined to PSHE/RSHE

All staff are expected to:

- Embed online safety into lessons and activities.
- Support students with search skills, critical thinking, and understanding legal issues (e.g. copyright, data protection).
- Reinforce safe use of generative AI tools and digital platforms.
- Use teachable moments to address online risks as they arise.

Review and Parental Engagement

- RSHE curriculum plans are reviewed annually to ensure alignment with statutory guidance.
- Parents and carers are kept informed about online safety education and encouraged to reinforce safe behaviours at home.

Safe use of technology

Device Misuse

Guildhouse School expects all students and staff to use school-issued and personal devices responsibly and in accordance with the school's Acceptable Use Policy. Misuse of devices, including accessing inappropriate content, bypassing security settings, engaging in online bullying, or using devices in ways that disrupt learning or compromise safety will be treated seriously. Students who misuse devices will be subject to the School Behaviour Policy, and staff will be held accountable under the Staff Code of Conduct. As part of our safeguarding approach, the school may restrict or revoke access to devices or digital platforms where necessary. All students sign the Student ICT Acceptable Use Agreement during induction, and expectations are reinforced regularly throughout the academic year.

Internet and search engines

- When using the internet, students should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate students are the ones who are most at risk.
- Students should not be allowed to aimlessly "surf" the internet and all use should have a clearly defined educational purpose.
- Despite filtering systems, it is still possible for students to inadvertently access unsuitable websites; to reduce risk, teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.

- Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the online safety coordinator, who will liaise with the IT team for temporary access. Teachers should notify the online safety coordinator once access is no longer needed to ensure the site is blocked.

Evaluating and using internet content

Teachers should teach students good research skills that help them maximise the resources available on the internet so that they can use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

Safe use of applications

- School email systems should be hosted by an email system that allows content to be filtered and allow students to send emails to others within the school or to approved email addresses externally.
- Social networking sites such as Facebook, Instagram and Twitter allow users to publish information about them to be seen by anyone who has access to the site. Generally, these would have limited use in the school, but students are likely to use these sites at home.
- Online communities and forums are sites that enable users to discuss issues and share ideas online.
- Chat rooms are internet sites where users can join in “conversations” on-line; Instant messaging allows instant communications between two people on-line. In most cases, students will use these at home although school internet systems do host these applications.
- Gaming-based sites allow students to “chat” to other gamers during the course of gaming. Many of the gaming sites are not properly moderated and may be targeted by adults who pose a risk to students. Consequently, such sites should not be accessible via school internet systems.

Safety rules

- Access to and use of personal email accounts, unregulated public social networking sites, chat rooms or gaming sites on the school internet system is forbidden and is usually blocked. This is to protect students from receiving unsolicited mail or contacts and to preserve the safety of the system from hacking and viruses.
- If the school identifies a clear educational use for emails or social networking sites and forums for on-line publishing, they should only use approved sites such as those provided by the IT service provider. Any use of these sites should be strictly supervised by the responsible teacher.
- Emails should only be sent via the school internet system to addresses within the School system or approved external address. All email messages sent by students in connection with school business must be checked and cleared by the responsible teacher.
- Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the online safety coordinator who will liaise with the learning platform provider.
- Student email addresses must not be published on the school website.
- Students should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

- Students should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites.
- All electronic communications should be polite; if a student receives an offensive or distressing email or comment, they should be instructed not to reply and to notify the responsible teacher immediately.
- Students should be warned that any bullying or harassment via email, chat rooms or social networking sites will not be tolerated and will be dealt with in accordance with the school's Behaviour Policy and Safeguarding Policy. This should include any correspondence or contact taking place outside the school and/or using non-school systems or equipment.
- Users should be aware that as use of the school internet system is for the purposes of education or school business only, and its use may be monitored.
- In order to teach students to stay safe online outside of school, they should be advised:
    1. not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended
    2. to only use moderated chat rooms that require registration and are specifically for their age group
    3. not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted as there is no control where images may end up or who can see them
    4. how to set up security and privacy settings on sites or use a "buddy list" to block unwanted communications or deny access to those unknown to them
    5. to behave responsibly whilst on-line and keep communications polite
    6. not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken
    7. not to arrange to meet anyone whom they have only met on-line or go "off-line" with anyone they meet in a chat room

Students own mobile devices

The majority of students are likely to have mobile phones or other devices that allows them to access internet services, and these can pose a major problem for the school in that their use may distract students during lessons and may be used for online bullying.

However, many parents prefer their students to have mobile phones with them in order to ensure their safety and enable them to contact home if they need to. Generally, use of personal mobile phones or other devices are forbidden in classrooms, unless used for educational purposes as directed by the teacher.

Social Media Incidents

At Guildhouse School, incidents involving social media are often safeguarding concerns and must be treated accordingly. Staff should follow the procedures outlined in the Safeguarding Policy when responding to any online behaviour that may pose a risk to a student's wellbeing.

Breaches involving students will be addressed under the School Behaviour Policy, while staff breaches will be managed in line with the Staff Code of Conduct.

Where an incident involves an inappropriate, upsetting, violent, or abusive social media post made by a member of the school community, the school will request that the post be removed and expects prompt action to be taken.

If the post originates from a third party outside the school community, the school may report it to the relevant platform and, where appropriate, escalate the matter to external agencies.

Responding to incidents

Policy statement

- All staff at Guildhouse School must recognise that online safety is an integral part of safeguarding.
- Any concern relating to online behaviour, content, or contact must be reported and managed in accordance with the Safeguarding and Child Protection Policy.
- Support staff, in particular, may be well-placed to notice early signs of concern in communal areas and corridors. Their vigilance and prompt reporting are essential to the school's safeguarding response.
- The school takes all reasonable steps to safeguard students online but acknowledges that incidents may arise both within and beyond the school environment. Online issues originating outside school can continue to affect students during the school day or over extended periods and must be treated with the same seriousness.
- All members of the school community are to report concerns swiftly to enable timely and sensitive investigation.
- Any suspected online risk or infringement must be reported to the Designated Safeguarding Lead (DSL) on the same day, with a written record made and sent directly via email in line with safeguarding procedures and safeguarding policy and recorded by the DSL using the form in accordance with appendix 1.
- Concerns or allegations involving staff misuse of technology must be referred directly to the Headteacher. Where the incident or complaint relates to a member of staff, the matter must always be referred to the Headteacher for action under staff conduct policies for low level incidents or consideration given to contacting the LADO under the CSCP guidance on dealing with allegations against staff where this is appropriate. Incidents involving the Headteacher are to be reported to the chair of the board of governors.
- The school will seek support from external agencies where appropriate, including the Local Authority, Prevent Officer, Police, or the UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH).
- In line with the DfE's Behaviour in Schools Guidance (September 2024), the school will follow best practice when responding to incidents involving child-on-child sexual harassment, online behaviour, and mobile phone misuse (pages 31–33 of the guidance).
- Parents and carers will be informed of online safety incidents involving their child, and the Police will be contacted where behaviour is considered unlawful or particularly concerning.
- The school's online safety coordinator is to keep a log of all online safety incidents and complaints and regularly review the information for evidence of emerging patterns of

individual behaviour or weaknesses in the school's online safety system and use these to update the online safety policy.

Although it is intended that online safety strategies and policies should reduce the risk to students whilst on-line, this cannot completely rule out the possibility that students may access unsuitable material on the internet. Neither the school nor the London Borough of Camden can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

The following sub-sections outline how specific types of online safety concerns are managed:

Sharing nudes and semi-nudes

Guildhouse School follows the UK Council for Internet Safety (UKCIS) guidance on incidents involving the sharing of nudes and semi-nudes with reference to the one-page summary titled *Sharing nudes and semi-nudes: how to respond to an incident*, which outlines immediate steps to take when such concerns arise.

It is often teaching staff or support staff who first become aware of these incidents. In such cases, staff must not view, copy, share, delete, or ask others to handle the imagery. Instead, they must report the concern directly to the Designated Safeguarding Lead (DSL) on the same day.

While the sharing of nudes involving children is illegal, students should be supported to speak openly and without fear of blame. The DSL will refer to the full guidance Sharing nudes and semi-nudes – advice for educational settings to assess the situation, determine whether external agencies need to be involved, and decide on appropriate next steps, including parental communication and student support.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child-on-child abuse students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying (which may also be referred to as cyberbullying), including incidents that take place outside of school should be treated like any other form of bullying and the school bullying policy should be followed. This includes issues arising from banter. Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence. Any action taken on online bullying incidents must be proportional to the harm caused. For some cases, it may be more appropriate to help the students involved to resolve the issues themselves rather than impose sanctions.

Action by service providers

All website providers and mobile phone companies are aware of the issue of online bullying and have their own systems in place to deal with problems, such as tracing communications. Teachers or parents can contact providers at any time for advice on what action can be taken.

- Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls. The student should also consider changing their phone number.

- Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced. The student should also consider changing email address.

- Where bullying takes place in chat rooms or gaming sites, the student should leave the chat room or gaming site immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.

- Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked.

- Parents are to be notified of any incidents (where appropriate) and advised on what measures they can take to block any offensive messages on computers at home.

Child-on-child sexual violence and sexual harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the guidance in KCSIE. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate.

Sexualised Online Behaviour

Guildhouse School recognises that the internet and social media platforms can be used to share sexually explicit content, which may be harmful, abusive, or constitute harassment and online bullying. Staff must be alert to online behaviours of a sexual nature that may pose safeguarding risks, including:

- Sharing explicit or unwanted content and images
- Consensual or non-consensual sharing of nude or semi-nude images (sexting)
- Upskirting
- Sexualised online bullying
- Unwanted sexual comments or messages
- Sexual exploitation, coercion, or threats
- Pressuring others to share images or perform sexual acts online

All staff have a duty to respond to such incidents in line with Keeping Children Safe in Education (KCSIE). The school must have clear procedures to manage online sexual harassment and recognise when behaviours may be linked to extra-familial harm, including criminal or sexual exploitation or gang-related activity. Any member of staff who becomes aware of such behaviour must report it to the Designated Safeguarding Lead (DSL) immediately.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. Guildhouse School recognises that extremist groups may use the internet to incite violence, promote hate, or share content related to terrorism. Some students may be vulnerable to radicalisation through direct contact with extremists or by self-radicalising after viewing extremist material online.

All staff have a statutory duty under the Prevent programme to help safeguard students from radicalisation. The primary referral mechanism is the Channel Panel, a multi-agency forum that supports at-risk individuals and helps divert them from extremism.

Staff must:

- Be aware of the school's Prevent duty and recognise signs of online radicalisation.
- Warn students about the risks of engaging with extremist content and reinforce that accessing such material breaches school policies.
- Report any concerns to the Designated Safeguarding Lead (DSL) immediately.

The school will:

- Maintain and regularly review filtering systems to block extremist content.
- Treat all incidents as breaches of the Acceptable Use Policy, applying behaviour or disciplinary procedures as appropriate.
- Ensure the DSL records MASH and reviews incidents to identify patterns or vulnerabilities.
- Refer concerns to the Local Borough Prevent Coordinator or Multi-Agency Safeguarding Hub if a student or their family is believed to be at risk.

Unintentional access of inappropriate websites

If a student or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the students' age, teachers should immediately (and calmly) close or minimise the screen.

Teachers should reassure students that they have done nothing wrong and discuss the incident with the class to reinforce the online safety message and to demonstrate the school's "no blame" approach.

The incident should be reported to the DSL/ online safety coordinator and details of the website address and URL provided.

The online safety coordinator should liaise with the network manager or learning platform provider to ensure that access to the site is blocked, and the school's filtering system reviewed to ensure it remains appropriate.

Intentional access of inappropriate websites by a student

If a student deliberately accesses inappropriate or banned websites, this constitutes a breach of the Student ICT Acceptable Use Agreement and will result in appropriate sanctions under the School Behaviour Policy.

The incident must be reported to the Designated Safeguarding Lead (DSL)/ Online Safety Coordinator, with the website address and URL recorded. The Online Safety Coordinator will liaise with the Network Manager or platform provider to ensure the site is blocked. Parents will be informed of the incident and the actions taken. The student will be reminded of the risks associated with accessing such material and supported to make safer choices online.

As part of ongoing online safety education, students are taught to:

- Share contact details only with trusted individuals.
- Limit access to their social media profiles to close friends.
- Avoid sending or posting inappropriate images.
- Not respond to offensive or harmful messages.
- Report concerns immediately to a trusted adult.

Risk from Inappropriate Contact with Adults Online

Guildhouse School recognises the serious safeguarding risks posed by inappropriate online contact between students and adults. This includes grooming, sexual exploitation, and abuse via messaging or video platforms.

Staff should be alert to:

- Students reporting or showing signs of inappropriate contact with adults online.
- Suspected grooming or plans to meet someone they've met online.
- Sexual abuse via video messaging, where perpetrators coerce students into performing sexual acts.

All concerns must be reported to the Designated Safeguarding Lead (DSL) immediately. The DSL will assess the situation, consult with the reporting staff member, and speak with the student if appropriate. If there is an immediate risk—such as a planned meeting—the DSL must contact the Police without delay.

The DSL may also seek advice from Camden's Online Safety Officer or Students Safeguarding and Social Work. Parents will be informed, where appropriate, and supported to help safeguard their child. Where school IT systems or networks are involved, the Online Safety Coordinator will work with the IT Manager to preserve evidence, audit systems, and minimise risk to other students.

Risk from sites advocating suicide, self-harm and anorexia

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- The school should ensure that young people have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PSHE/RSHE curriculum.
- Pastoral and Welfare support can be made available to any students to discuss issues affecting them and to establish whether their online activities are an added risk factor.

- Staff receive ongoing training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.

Use of generative AI

At Guildhouse School, we acknowledge that generative AI platforms (e.g. ChatGPT or Gemini for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. Guildhouse School is aware of and follows the DfE's guidance on this.
In particular:

  - We discuss the use of these tools with students and staff, including their practical use as well as their ethical pros and cons.
  - We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students, these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, nudifying apps and inappropriate chatbots).
- The use of any generative AI in Exams, or to plagiarise and cheat is prohibited, and the Behaviour Policy will be used for any student found doing so.

Searching and Confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools and school's policy, the Headteacher and staff authorised by them have a statutory power to search students/property on school premises. This includes the content of mobile phones and other devices, for example because of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Appropriate filtering and monitoring

The designated safeguarding lead (DSL) has lead responsibility for filtering and monitoring and works closely with IT Support to implement the DfE filtering and monitoring standards, which require schools to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs.

Guildhouse School provides appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times. All staff are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point via email or contacting the DSL directly on Microsoft Teams.

The Central IT Team, Safeguarding Governor and safeguarding colleagues work together closely to carry out annual reviews and check and also to ensure that the school responds to issues and integrates with the curriculum.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well and regular training reminders

The DSL checks filtering reports, monitoring alerts and notifications on a daily basis and takes any necessary action as a result.

At Guildhouse School, Securly is used, which is a cloud-based web filtering system, to safeguard students across all devices. Securly helps ensure compliance with KCSIE and Prevent Duty by blocking access to inappropriate, harmful, or extremist content in real time.

Data protection

Data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, it's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child. And in KCSIE 2025, The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children.

Monitoring and Review

Guildhouse School is committed to maintaining a robust and responsive approach to online safety. This policy will be reviewed annually, or sooner if significant changes occur in statutory guidance, technology use, or safeguarding practice. The Online Safety Coordinator/Designated Safeguarding Lead (DSL) and Senior Leadership Team, will monitor the effectiveness of online safety measures, including filtering systems, incident reporting procedures, and curriculum delivery. Feedback from staff, students, and parents will inform updates to ensure the policy remains relevant, practical, and aligned with the school's safeguarding priorities.

Related Policies

Safeguarding and Child Protection Policy
Anti-Bullying Policy
Student Behaviour Policy
Prevent Strategy and Risk Assessment

Statutory guidance links as referenced throughout policy

1. Keeping Children Safe in Education (KCSIE) 2025

- KCSIE 2025 Full Guidance (PDF)
- KCSIE GOV.UK Overview Page [www.gov.uk]

2. UKCIS Guidance – Sharing Nudes and Semi-Nudes

- Full UKCIS Guidance (PDF) [assets.pub...ice.gov.uk]
- One-Page Summary for Staff

3. DfE Behaviour in Schools Guidance (Feb 2024)

- Behaviour in Schools: Advice for Headteachers and Staff (PDF)
- Behaviour in Schools GOV.UK Page

4. Prevent Duty Guidance

- Prevent Duty: Safeguarding Learners (GOV.UK)
- Prevent Duty Guidance for England and Wales (PDF)

5. DfE Filtering and Monitoring Standards

- Filtering and Monitoring Standards for Schools and Colleges

6. DfE Generative AI in Education Guidance

- Generative AI in Education Policy Paper
- Safe Use of Generative AI – Module 3

7. Statutory RSE and Health Education Guidance

- RSE and Health Education Guidance (2025 Update)

Appendices

Appendix 1: Online Safety Incident Report Form

Name of School/organisation:	Guildhouse School London
Address:	43-45 Bloomsbury Square, Holborn, WC1A 2RA
Name of online safety coordinator:	Jamie Forbes
Contact details:	jforbes@guildhouseschool.com

Details of Incident

Date happened:	
Time:	
Name of person reporting incident:	
(If not reported, how was the incident identified?)	
Where did the incident occur?	□ In school/service setting
	□ Outside school/service setting
Who was involved in the incident?	□ child/young person
	□ staff member
	□ other (please specify below)
Type of incident:	□ bullying or harassment (online bullying)
	□ deliberately bypassing security or access
	□ hacking or virus propagation

	□ racist, sexist, homophobic, transphobic, bi-phobic, religious hate material
	□ terrorist material
	□ online grooming
	□ online radicalisation
	□ child abuse images
	□ on-line gambling
	□ soft core pornographic material
	□ illegal hard core pornographic material
	□ other (please specify below)

Description of Incident

Nature of Incident

□ **Deliberate Access**	
Did the incident involve material being:	□ Created
	□ Viewed
	□ Printed
	□ Shown to others
	□ Transmitted to others
	□ Distributed
Could the incident be considered as:	□ harassment
	□ grooming
	□ online bullying
	□ breach of AUP
□ **Accidental Access**	
Did the incident involve material being:	□ Created
	□ Viewed
	□ Printed
	□ Shown to others
	□ Transmitted to others
	□ Distributed

Action Taken

□ **Staff**	□ incident reported to Headteacher/senior manager
	□ advice sought from LADO
	□ referral made to LADO
	□ incident reported to police

	□ incident reported to Internet Watch Foundation
	□ incident reported to IT
	□ disciplinary action to be taken
	□ online safety policy to be reviewed/amended
	Please detail any specific action taken (i.e.: removal of equipment, below)
□ **Child / Student / Young Person**	□ incident reported to Headteacher/senior manager
	□ advice sought from Students Safeguarding and Social Work
	□ referral made to Students Safeguarding and Social Work
	□ incident reported to police
	□ incident reported to social networking site
	□ incident reported to Internet Watch Foundation
	□ child's parents informed
	□ disciplinary action to be taken
	□ child/young person debriefed
	□ online safety policy to be reviewed/amended
	Please detail any specific action taken (i.e.: removal of equipment, below)

Outcome of Incident / Investigation

GUILDHOUSE SCHOOL
LONDON