

The American School in London

Online Safety Policy

The current version of any policy, procedure, protocol or guideline is the version held on the ASL website. It is the responsibility of all employees to ensure that they are following the most up-to-date version.

Responsible parties	Director of Technology Designated Safeguarding Lead
Approved by	Buildings & Grounds Committee
Approval date	May 2026

1. Aims and Objectives

It is the duty of The American School in London to ensure that every student in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning, but also pose great risks to young people. Our students are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalization and identity theft.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites
- Email and instant messaging
- Blogs, forums and chat rooms
- Mobile internet devices such as smart phones and tablets
- Social networking sites
- Music / video downloads
- Gaming sites and online communities
- Instant messaging technology via SMS or social media sites
- Video calls

- Podcasting and mobile applications
- Virtual and augmented reality technology
- Artificial intelligence

This policy, supported by the Responsible Use Agreements for employees and students, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimize risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding and Child Protection Policy
- Responsible Use Agreements (employees and students)
- Data Protection Policy
- Behavior Policy
- Anti-Bullying Policy
- Web Filtering Rules
- AI Policy for Employees and AI Policy for Students

At The American School in London, we understand the responsibility to educate our students on online safety issues; teaching them the appropriate behaviors and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving students in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

2. Scope

This policy applies to all members of the school community, including staff, students, parents and visitors, who have access to and are users of the school IT systems. In this policy:

- "staff" includes teaching and non-teaching employees, contractors and volunteers
- "parents" includes students' carers and guardians
- "visitors" includes anyone else who comes to the school including alumni.
- "Students" includes all currently enrolled students including those in the summer program.

Both this policy and the Responsible Use Agreements cover both fixed and mobile internet devices provided by the school (such as desktops, laptops, tablets, digital video equipment, etc.); as well as all devices owned by students, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

In designing this policy, the school has considered the "4Cs" outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. However, the school recognizes that many students will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some students may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at school. The improper use of mobile technology by students, in or out of school, will be dealt with under the school's Behavior Policy and/or Safeguarding and Child Protection Policy as is appropriate in the circumstances.

3. Roles and Responsibilities in Relation to Online Safety

All staff and visitors have responsibilities under the Safeguarding and Child Protection Policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in line with the Safeguarding and Child Protection Policy.

3.1 The Board of Trustees

The Board of Trustees has overall leadership responsibility for safeguarding as outlined in KCSIE and ASL's Safeguarding and Child Protection Policy. The Board of Trustees is responsible for the approval of this policy and for reviewing its effectiveness at least annually.

The Board of Trustees will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- All staff, in particular the Designated Safeguarding Lead and Senior Leadership Team are adequately trained about online safety
- All staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to escalate concerns when identified
- Staff are aware of the school procedures and policies that should be followed in the event of abuse or suspected breach of online safety in connection to the school

3.2 Head of School and the Senior Leadership Team

The Head of School is responsible for the safety of the members of the school community and this includes responsibility for online safety. Together with the Senior Leadership Team, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

3.3 The Designated Safeguarding Lead (DSL)

The DSL takes the lead responsibility for Safeguarding and Child Protection at The American School in London. This includes a responsibility for online safety as well as the school's filtering and monitoring system.

The DSL will ensure that this policy is upheld at all times, working with the Head of School, Senior Leadership Team, and TILM Department (Technology, Information Literacy, and Media) to achieve this. As such, in line with the Safeguarding and Child Protection Policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

The DSL will work closely with the Director of Technology and the TILM Department to ensure that the school's requirements for filtering and monitoring are met and enforced. The DSL will review filtering and monitoring reports and ensure that checks are properly made of the system at least annually and more frequently if needed.

3.4 Online Safety Coordinator

The DSL will hold the role of Online Safety Coordinator in collaboration with the Director of Technology. They will keep up to date on current online safety issues and guidance issued by relevant organizations, including the Department for Education (including KCSIE), Independent Schools Inspectorate (ISI), the CEOP (Child Exploitation and Online Protection), Childnet International and Local Safeguarding Children Procedures. The Online Safety Coordinator will monitor any disclosure, report or suspicion of improper use of school IT or any issues with the school's filtering and monitoring system.

3.5 TILM Department (Technology, Information Literacy, and Media)

The school's TILM Department Technology Staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the Online Safety Coordinator.

3.6 Teaching and Support Staff

All staff are required to sign and return the Responsible Use Agreement before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

All teaching staff are required to use the school's Resource Review procedures to vet and deliver digital resources including educational videos. This includes a standing recommendation, where possible, to embed approved YouTube videos into teaching platforms rather than using direct links, ensuring a controlled and focused learning experience for students.

All staff must read and understand this Online Safety Policy and enforce it in accordance with direction from the DSL and the Head of School/Senior Leadership Team as appropriate.

In accordance with the Safeguarding and Child Protection Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's DSL.

3.7 Students

Students are responsible for using the school IT systems in accordance with the Responsible Use Agreement for students and Student Code of Conduct.

3.8 Parents and Carers

The American School in London believes that it is essential for parents to be fully involved with promoting online safety at home. We discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will contact parents if it has any concerns about students' behavior in this area and likewise it hopes that parents will feel able to share any concerns with the school.

4. Filtering and Monitoring

4.1 In General

The American School in London is committed to providing a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Staff, students, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access prohibited or inappropriate content, or attempting to circumvent

the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behavior Policy, as appropriate.

The Online Safety Coordinator will check at least annually (and more often if needed) that the filtering and monitoring systems are operating effectively – these checks must be recorded along with any appropriate action. The Safeguarding and/or Online Safety representative from the Board of Trustees, the DSL and Director of Technology will review the filtering and monitoring system regularly. Such a review should occur before the beginning of every new academic year; however, such reviews should also occur if:

- There is a major safeguarding incident
- There is a change in working practices
- Any new technology is introduced

4.2 Filtering System

The school's filtering system uses **Fortigate network filtering** with **FastVue reporting** to block internet access to harmful sites and inappropriate content. The filtering system will block access to the following categories of websites:

- Child sexual abuse material
- Suicide
- Self-harm
- Terrorism
- Extremist Violence/Content
- Explicit violence
- Illegal or Unethical Content
- Weapons/Weapons Sales
- Hacking
- Drug Abuse
- Pornography
- Adult Content
- Nudity
- Discrimination
- Gambling
- Proxy Avoidance
- Plagiarism
- Cryptocurrency
- Brokerage and Trading
- Peer-to-peer file sharing
- Dating
- Social media
- Instant Messaging
- Games
- Artificial Intelligence

We maintain an allow list for exceptions to blocked content by request and approval of staff and for educational purposes. If there is a good educational reason why a particular website, application, or form of content should not be blocked, a student should contact the relevant member of teaching staff, who will then contact the TILM Department or DSL for their consideration.

4.3 Monitoring System

The school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server, allowing individuals to be identified (as described in sections 3.3, 3.4 and 3.5). Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify the TILM Department if they are teaching material which might generate unusual internet traffic activity.

4.4 Staff Responsibilities

If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify the TILM Department if they believe that appropriate teaching materials are being blocked and if inappropriate content is accessible.

4.5 Student Responsibilities

Students must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to the DSL, a teacher, TILM Department, or trusted adult at school. Deliberate access to any inappropriate materials by a student will be addressed pursuant to the school's Behavior Policy. Students should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work/research purposes, students should contact a member of the TILM Department Technology Staff.

4.6 Educational Videos

We recognize that while educational video platforms (such as YouTube) are valuable learning resources, unrestricted access can be distracting or irrelevant to education objectives. To balance utility with safety and focus, we implement the following:

- **Content Filtering:** The school enforces YouTube content restriction across the network and on all school-issued devices. Filtering is applied in a tiered manner, taking into account age-appropriate content categories rather than relying solely on restrictions for adult (18+) content. These settings are reviewed periodically, and additional restrictions may be applied where feasible to support student safety and focus.
- **Curated Access:** We require teachers to use existing Resource Review procedures to select and share appropriate video content. Where possible, approved videos should be embedded directly within school-approved teaching platforms to minimize exposure to external content and distractions. However, in cases where embedding is not technically possible (for example, where embedding is disabled by the content owner), teachers may provide direct links to the approved video, while continuing to apply professional judgement and oversight.

5. Education and Training

5.1 Staff: Awareness and Training

As part of their induction, all new staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviors in their classrooms and following the school's Online Safety procedures. Teachers are encouraged to collaborate with TILM co-teachers for instructional support to plan and teach digital citizenship and online safety in their courses.

All staff receive training once a year and regular information on online safety issues in the form of professional development and meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. Staff training will include a specific focus on staying current on the guidelines and expectations for using educational video platforms, in particular reviewing what YouTube videos are used and where they are hosted.

Teaching staff are required, with TILM support, to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They are responsible to know what to do in the event of misuse of technology by any member of the school community. When students use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

5.2 Students: The Teaching of Online Safety

Online safety guidance will be given to students on a regular basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our students' understanding of it.

The school provides opportunities to teach about online safety within a range of curriculum areas and TILM lessons. Educating students on the dangers of technologies that may be encountered outside school will also be carried out via advisory programs, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, students are taught about their online safety responsibilities and to look after their own online safety. From Grade 7, students are formally taught about recognizing online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Additionally students are taught about misinformation, disinformation and conspiracy theories that are propagated online. Students can report concerns to the DSL and any member of staff at the school.

From grade 4, students are also taught about relevant laws applicable to using the internet such as those that apply to data protection, online safety and intellectual property. Students are taught about respecting other people's information and images through discussion and classroom activities.

Students should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Safeguarding and Child Protection and Anti-Bullying Policies, which describe the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Students should approach the DSL, or any other member of staff they trust, as well as parents and peers for advice or help if they experience problems when using the internet and related technologies.

5.3 Parents

The school seeks to work closely with parents and guardians in promoting a culture of online safety. The school will contact parents if it has any concerns about students' behavior in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognizes that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore arranges informational evenings for parents when an outside specialist advises about online safety and the practical steps that parents can take to minimize the potential dangers to their children without curbing their natural enthusiasm and curiosity.

6. Use of School and Personal Devices

6.1 Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorized people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device, staff should ensure that it is locked to prevent unauthorized access. Devices issued to staff are encrypted to protect data stored on them.

Staff at The American School in London are permitted to bring in personal devices for their own use. Staff may use such devices during personal time (break-times and lunchtimes) and not while teaching or in student-facing roles. It is highly recommended that personal devices are out of sight when not used and are password protected.

Any temporary use of a personal device to capture student images/videos, where necessary, must strictly adhere to the immediate transfer and deletion procedures outlined in the [Guidelines for the Use of Images of Children](#), which mandates immediate transfer to a school-approved platform and immediate deletion from the personal device and all back-up locations. Please read this in conjunction with the Safeguarding and Child Protection Policy, Responsible Use Agreements, and related school policies.

6.2 Students

Students are not permitted to use mobile phones between 8:00 AM and 3:00 PM. Mobile phones must be put away for high school students during the school day. Mobile phones cannot be brought to campus for lower and middle school students. See divisional expectations for more information.

The school requires high school students to use student-owned laptops through a 1:1 BYOD program as a teaching and learning tool. For younger students, the school provides devices for on-campus use in grades K1 through Grade 5, and school-issued laptops for grades 6 through 8 that are taken home throughout the school year. Students are required to adhere to the Responsible Use Agreement when using personal devices for school work. In particular, the Responsible Use Agreement requires students to ensure that their use of devices for school work complies with this policy and prohibits students from using devices for non-school related activities during the school day.

School mobile technologies made available for student use by the school (including laptops, tablets, cameras, etc.) are stored securely. Access is managed by teachers and TILM Department Technology Staff. Members of staff should sign devices out and in before and after each use by a student.

Students are responsible for their conduct when using school issued or their own devices. Any misuse of devices by students will be dealt with under the School's Behavior Policy.

The school recognizes that mobile devices are sometimes used by students for medical purposes or as an adjustment to assist students who have disabilities or special educational needs. Where a student needs to

use a mobile device for such purposes, the student's parents or carers should arrange a meeting with the appropriate member of the leadership team to agree how the school can appropriately support such use. The designated person will then inform the student's teachers and other relevant members of staff about how the student will use the device at school.

7. Online Communications

7.1 Staff

Any digital communication between staff and students or parents/carers must be professional in tone and content. Under no circumstances may staff contact a student or parent/carer using any personal email address or SMS/WhatsApp. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details, may not be shared with students or parents/carers. Under no circumstances may staff contact a student or parent/carer using a personal telephone number, email address, or other messaging system, nor should students or parents/carers be added as social network 'friends' or similar.

Staff must immediately report to the DSL/Head of School the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the TILM Department Technology Staff.

7.2 Students

All students are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work, assignments, research and projects. Students should be aware that email communications through the school network and school email addresses are monitored.

The school will ensure that there is appropriate and strong IT monitoring and antivirus software. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work/research purposes, students should contact the TILM Department Technology Staff for assistance.

Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to a member of staff who should then refer it to the DSL.

8. Use of Social Media

8.1 Staff

Staff must not access social networking sites or personal email from school devices whilst teaching or in student-facing roles. Such access may be made from staff members' own devices during personal time (break-times and lunchtimes) in staff-only areas of school. In addition, and as stated in the ASL Code of Conduct, ASL personnel should not friend ASL alumni within four years of the alumnus or alumna's

graduation from ASL, and should always use their discretion when connecting with alumni and parents using social media.

When accessed from staff members' own devices or off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school. Staff should apply appropriate privacy settings on social media accounts

Any online communications, whether by email, social media, private messaging or other, must not:

- Place a child or young person at risk of, or cause, harm
- Bring The American School in London into disrepute
- Breach confidentiality
- Breach copyright
- Breach data protection legislation
- Do anything that could be considered discriminatory against, or bullying or harassment of, any individual on the basis of protected characteristics under the UK Equality Act 2010 for example by:
 - Making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age
 - Using social media to bully another individual
 - Posting links to or endorsing material which is discriminatory or offensive
- Otherwise breach the Responsible Use Agreement or Safeguarding and Child Protection Policy

8.2 Students

The school expects students to think carefully before they post any information online, or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The school takes misuse of technology by students very seriously and incidents will be dealt with under the Behavior Policy, Safeguarding and Child Protection Policy, and Anti-Bullying Policy as appropriate.

9. Data Protection

Please refer to the Data Protection Policy and the Responsible Use Agreements for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.

Staff and students are expected to save all data relating to their work to their school-issued devices or to the school's approved cloud storage systems as per the Responsible Use Agreements.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorized to do so, and only when it is necessary and required in order to fulfill their role. No personal data of staff or students should be stored on personal devices.

Staff should also be particularly vigilant about scam/phishing emails (and similar) which could seriously compromise the school's IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the TILM Department Technology Staff in accordance with the Data Protection Policy and Responsible Use Agreements.

Any security breaches or attempts, loss of equipment and any unauthorized use or suspected misuse of IT must be immediately reported to the Helpdesk or a member of the TILM Department.

10. Password Security

Students and staff have individual school network logins, email addresses and storage folders on the server. Staff and students are regularly reminded of the need for password security as outlined in the Responsible Use Agreements and [ASL Password Change page](#).

11. Safe Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. Staff must also all adhere to the school's policy of honoring parents' consent to publishing their children's images on external or public-facing websites and social media.

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognize the risks attached to publishing their own (personal) images on the internet (e.g. on social networking sites) and follow the school's policy on official social media posting.

12. Artificial Intelligence (AI)

The American School in London has developed a comprehensive approach to artificial intelligence in education, which is detailed in our separate AI Policy. This Online Safety Policy addresses AI primarily from the perspective of online safety and appropriate use.

12.1 General Principles

Only school-approved AI tools may be used on school devices and systems. AI categories are generally blocked on our network except for those specifically approved for educational use. This approach is in line with the Department for Education's guidance that "Pupils should only be using generative AI in education settings with appropriate safeguards in place, such as close supervision and the use of tools with safety and filtering and monitoring features."

12.2 Student Use of AI

For students, the following AI tools are permitted:

- Flint, Canva, Adobe Firefly
- Other AI tools may be used only with explicit teacher permission, supervision and after review and approval of the TILM department.

The following AI tools are blocked for student use:

- ChatGPT, Google Gemini, Perplexity, Claude
- Other general-purpose AI chatbots not specifically approved by the school

12.3 Staff Use of AI

Employees have access to a broader range of AI tools, including Google Gemini, for professional use. Staff should use AI tools responsibly and in accordance with the school's AI Policy and Responsible Use Agreement.

12.4 Data Privacy and AI

Personal or confidential information should not be entered into generative AI tools. This technology can potentially store and/or learn from data inputted and users should consider that any information entered into such tools may be released to the internet or used for training AI models.

Note: Some AI tools licensed for use within the school's broader digital ecosystem, such as Flint and Gemini, offer assurances that input data will not be used externally or for training. However, users should still exercise caution when entering sensitive information.

12.4 Accuracy and Critical Thinking

It is important to be aware that AI technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for complete accuracy. In particular:

- Students should not use these tools to answer questions about health, medical, or wellbeing issues, or indeed anything of a personal nature
- Students should be encouraged to verify AI-generated information through reliable sources
- It is always best to seek help and recommendations as to reliable resources from a member of staff or the DSL

12.4 Reference to Comprehensive AI Policy

For detailed guidance on:

- Appropriate uses of AI in teaching and learning
- Academic integrity and AI
- Assessment policies related to AI use
- Specific protocols for different AI tools
- Professional development related to AI

Please refer to the school's separate AI Policies.

13. Misuse

The American School in London will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the school will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they should report it to the DSL. The DSL may seek assistance from CEOP, the LADO, and/or professional advisers as appropriate.

The school will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our Safeguarding and Child Protection and Behavior policies.

14. Complaints

As with all issues of safety at The American School in London, if a member of staff, a student or a parent/carer has a complaint or concern relating to online safety, prompt action will be taken to address it. Complaints should be addressed to the DSL in the first instance, who will liaise with the senior leadership team and undertake an investigation where appropriate. Please see the school's Complaints Policy for further information.

Incidents of, or concerns around online safety will be recorded in accordance with the Safeguarding and Child Protection Policy and reported to the school's DSL in accordance with the school's Safeguarding and Child Protection Policy.