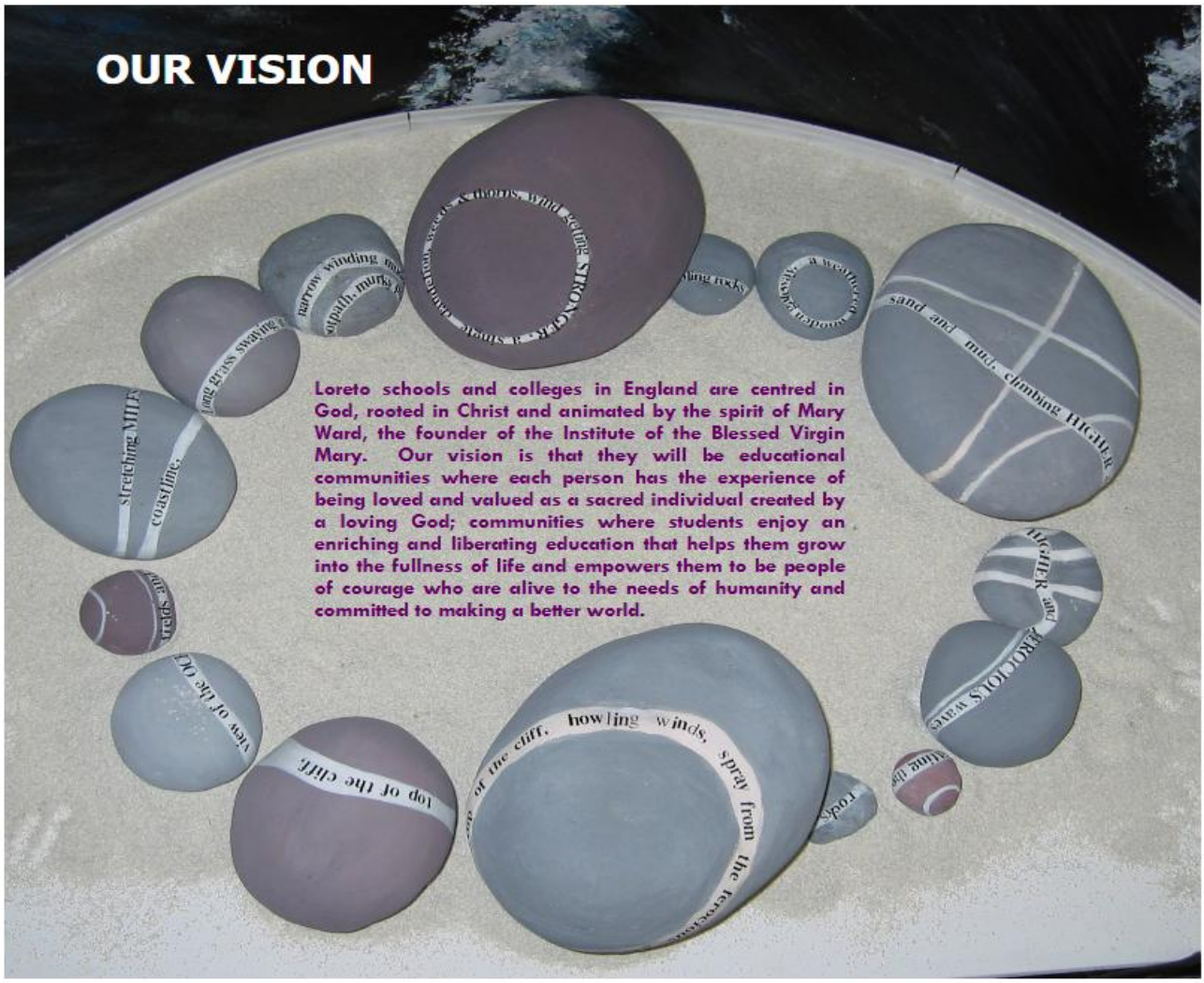
ONLINE SAFETY POLICY

Date of revised policy approval	September 2026
Next review date	September 2027
Distribution to	All Staff
Owner of policy	Mrs Walker, Deputy Headteacher
Approved by	Curriculum Governors Committee
Reviewed and prepared by	Mrs N Walker and Ms H Greene
Location of policy	School Network

OUR VISION


OUR VISION
Loreto schools and colleges in England are centred in God, rooted in Christ and animated by the spirit of Mary Ward, the founder of the Institute of the Blessed Virgin Mary. Our vision is that they will be educational communities where each person has the experience of being loved and valued as a sacred individual created by a loving God; communities where students enjoy an enriching and liberating education that helps them grow into the fullness of life and empowers them to be people of courage who are alive to the needs of humanity and committed to making a better world.
sand and mud, climbing HIGHER
HIGHER and HIGHER waves
top of the cliff,
view of the cliff,
howling winds, spray from the

OUR MISSION STATEMENT

I am the Way

The Truth

And

The Life

(John 14:6)

At Loreto Grammar School Altrincham, students, staff, parents and Governors form a Catholic community. We aspire to create a caring, structured environment in which teaching and learning and the experience of school

- are characterised by joyful and loving service to others
- challenge each of us to realise our full potential in a spirit of joy and creativity
- encourage the pursuit of excellence
- uphold honesty, justice and mutual respect
- enable us to be questioning, independent learners and "seekers of truth"
- prepare each of us to meet with confidence the challenges of a changing world
- improve and enrich the life of the wider community and enable us to be an example of Christian values in the world as witnesses to God's Living Kingdom

Our values are centred in God, rooted in gospel values and derive from the vision of Mary Ward.

Love and speak the truth – at all times

(Mary Ward)

Loreto Grammar School Online Safety Policy

Loreto Grammar School understands that using online services is an important aspect of raising educational standards, promoting student achievement and enhancing teaching and learning.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of students and staff.

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

- Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- Contact: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- Commerce: Risks such as online gambling, inappropriate advertising, phishing, and financial scams.

The measures implemented to protect students and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

Online safety is recognised as a whole-school safeguarding responsibility. The school understands that many safeguarding concerns now have an online dimension and that online safety underpins the school's safeguarding culture.

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2026) 'Keeping children safe in education'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- Voyeurism (Offences) Act 2019
- UK Council for Child Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' (current edition)

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Cyber Security Policy (Examinations)
- Staff and Student IT Acceptable Use Policy
- Safeguarding and Child Protection Policy
- RSE and Health Education Policy
- Staff Code of Conduct
- Behaviour Policy

- Disciplinary Policy and Procedures
- Data Protection Policy
- Remote Learning Procedures
- External Speakers and Resources Guidance
- Prevent Risk Assessment

Roles and responsibilities

The Governing Body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training (including online safety) at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that a named safeguarding governor has strategic oversight of filtering and monitoring systems and receives regular reports regarding their effectiveness.
- Ensuring that filtering and monitoring systems are reviewed at least annually, and following any safeguarding incident, with documented evidence of review.

The Headteacher is responsible for:

- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and governing body to update this policy on an annual basis.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the IT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to

update the school's procedures.
- Reporting to the Governing Body about online safety.
- Reviewing monitoring alerts and reports (or delegating this responsibility appropriately), ensuring safeguarding concerns are triaged and acted upon in accordance with the Safeguarding and Child Protection Policy.
- Ensuring that online safety concerns are considered within the context of wider safeguarding risks, including contextual safeguarding and early help intervention where appropriate.
- Working with the Headteacher and Governing Body to update this policy on an annual basis.

The Network Manager and IT technicians are responsible for:
- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

Heads of department are responsible for:
- Ensuring that where appropriate, online safety is taught in their curriculum.
- Ensuring that all technologies used in the department are appropriate.
- Supporting staff in their departments to adhere to the policy.

All staff members are responsible for:
- Taking responsibility for the security of IT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Exercising caution with the use of artificial intelligence. Follow the Data Protection Policy and legal requirements around the use of personal and identifiable data.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Students are responsible for:
- Adhering to this policy, the IT Acceptable Use Policy and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Exercising caution with the use of artificial intelligence. Follow the Data Protection Policy and legal requirements around the use of personal and identifiable data.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

The curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSE
- PSHE
- Computer science
- Form period, including Sixth Form

The curriculum and the school's approach to online safety is developed in line with Keeping Children Safe in Education, the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance.

Students are taught the underpinning knowledge and behaviours that can help them navigate the online world safely and confidently regardless of the device, platform or app they are using.

Online safety teaching is always appropriate to students' ages and developmental stages. The underpinning knowledge and behaviours students learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support

The online risks students may face online are always considered when developing the curriculum. Keeping Children Safe in Education (2026) identifies four key areas of online risk which inform the school's curriculum and safeguarding approach:

- 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 or generative AI applications that simulate this; 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: 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, including those generated or altered using artificial intelligence, and/or pornography), sharing other explicit images and online bullying.
- Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The DSL is involved with the development of the school's online safety curriculum.

The school recognises that, while any student can be vulnerable online, some pupils may be more susceptible to online harm or have less support in staying safe online, including pupils with SEND, looked after children, those with mental health needs, and those at risk of exploitation. These pupils may receive additional targeted support where appropriate.
Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of students. When reviewing these resources, the following questions should be asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age appropriate for students?
- Are they appropriate for students' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate. The DSL will make relevant staff members aware of any student who has suffered, or may be suffering from online abuse or harm, and advise them on how best to support the student.

Lessons and activities are planned carefully so they do not draw attention to a student who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which students feel comfortable to say what they feel and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything students raise during online safety lessons and activities, they will log this via CPOMS.

If a student makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will log this via CPOMS.

Staff training

All staff receive safeguarding and child protection training, which includes online safety training, during their induction. All staff receive a copy of this policy upon their induction and are informed of any changes to the policy. The Teacher's Standards: Part Two – Personal and Professional Conduct should be referred to at all times and underpins staff responsibility.

Online safety updates are provided annually and are delivered in line with advice from the three local safeguarding partners.

Staff are required to adhere to the Staff Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media.

Staff must report to the DSL any incidences of students attempting to add them to their social media accounts.

All staff are informed about how to report online safety concerns via CPOMS.

The DSL and IT technicians act as the first points of contact for staff requiring advice about online safety.

Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:

- Parents' wellbeing evenings
- Newsletters/bulletins
- Emails

Parents are sent a copy of the IT Acceptable Use Policy at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Classroom use

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Intranet
- Cameras

- Student devices
-

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that students use these platforms at home, the class teacher always reviews and evaluates the resource. Students are supervised when using online materials during lesson time, this supervision is suitable to their age and ability.

Internet access

Students, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the IT Acceptable Use Policy.

The Governing Body ensures the school's IT network has appropriate filters and monitoring systems in place. The IT technicians undertake a risk assessment to determine what filtering and monitoring systems are required.

The filtering and monitoring systems the school implements are appropriate to students' ages, the number of students using the network, how often students access the network, and the proportionality of costs compared to the risks.

Filtering and monitoring systems are reviewed at least annually, and following any safeguarding incident, by the DSL,

Network Manager and the named safeguarding governor. Records of these reviews are maintained. The needs of the filtering system are dynamic and therefore extra filters and the blocking of sites happens where required to ensure that the services are safe and appropriate for all users.

Monitoring reports and alerts are reviewed regularly by the DSL and/or delegated safeguarding staff. Safeguarding concerns identified through monitoring are triaged promptly and managed in accordance with the Safeguarding and Child Protection Policy.

The IT technician ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

IT technicians undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate. Requests regarding making changes to the filtering system are directed to the Headteacher. Reports of inappropriate websites or materials are made to an IT technician immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and IT technicians, who will escalate the matter appropriately. If a student has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Management Policy. This includes the use of Virtual Private Networks (VPN) using the school WiFi systems or any other such system.

If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the relevant school policies.

Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by the Network Manager and IT technicians. Firewalls are switched on at all times. Staff and students are advised not to download unapproved software or open unfamiliar email attachments. Staff members and students are advised to report all malware and virus attacks to IT technicians.

All members of staff and students have their own unique usernames and private passwords to access the school's systems and are responsible for keeping them private at all times. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. Users are required to lock access to devices and systems when they are not in use. Users inform IT technicians if they forget their login details and arrangements are made for the user to access the systems under different login details. If a user is found to be sharing their login details or otherwise mistreating the password system, the IT technician is informed and the account is temporarily suspended. The relevant school policy is then implemented.

Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Access to and the use of emails is managed in line with the IT Acceptable Use Policy. Staff and students are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Personal email accounts are not permitted to be used on the school site.

Any email that contains sensitive or personal information is only sent using secure or passworded/encrypted email.

The school's monitoring system can detect inappropriate links, malware and profanity within emails; staff and students are made aware of this.

Chain letters, spam and all other emails from unknown sources are deleted without being opened.

Any cyberattacks initiated through emails are managed in line with the Data and E-Security Breach Prevention and Management Plan.

Social networking – Personal use

Access to social networking sites is filtered as appropriate. Staff and students are not permitted to use social media for personal use during lesson time. Staff and Sixth Form can use personal social media during break and lunchtimes; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action.

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. Staff are not permitted to communicate with students over social networking sites and are reminded to alter their privacy settings to ensure students are not able to contact them on social media.

Students are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behaviour Management Policy.

Social networking – Use on behalf of the school

The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the Headteacher to access to the school's social media accounts. All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

The school website

The Headteacher is responsible for the overall content of the school website; they will ensure the content is appropriate, accurate, up-to-date and meets government requirements. The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and students is not published on the website.

Images and videos are only posted on the website if consent has been given by parents/carers.

Use of school-owned devices

Staff members may be issued with the following devices to assist with their work:

- Laptop
- Phone
- iPad

Students may be provided with school-owned devices as necessary to assist in the delivery of the curriculum. School-owned devices are used in accordance with the IT Acceptable Use Policy. Staff and students are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected.

All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased. IT technicians review all school-owned devices on a regular basis to carry out software updates and ensure there is no inappropriate material on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from IT technicians.

Staff members or students found to be misusing school-owned devices are disciplined in line with the Disciplinary Policy and Procedure and Behaviour Management Policy.

Use of personal devices

Personal devices are used in accordance with the IT Acceptable Use Policy. Any personal electronic device that is brought into school is the responsibility of the user.

Personal devices are not permitted to be used in the following locations:

- Toilets
- Changing rooms

Staff members are not permitted to use their personal devices to take photos or videos of students.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Disciplinary Policy and Procedure. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the Headteacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Procedure.

Students are not permitted to use their personal devices when moving between lessons or during lesson time unless they have permission from the teacher. If a student needs to contact their parents during the school day, they are able to go to Student Services. Students' devices can be searched, screened and confiscated in accordance with the Behaviour Management Policy. If a staff member reasonably believes a student's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

The use of Virtual Private Networks (VPN) or any other such systems to bypass the School security system is not permitted by staff or students on personal devices when using the School WiFi system.

Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

Managing reports of online safety incidents

Staff members and students are informed about what constitutes inappropriate online behaviour. This is done via:

- Staff training
- The online safety curriculum
- Assemblies

Concerns regarding a staff member's online behaviour are reported to the Headteacher who decides on the best course of action in line with the relevant school policies, e.g. Staff Code of Conduct and Disciplinary Policy and Procedures.

Concerns regarding a student's online behaviour are reported to the DSL via CPOMS who investigates concerns with relevant staff members. Concerns regarding a student's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. Behaviour Management Policy, Safeguarding and Child Protection Policy.

Concerns about staff online behaviour that do not meet the threshold for referral to the Local Authority Designated Officer (LADO) will be managed in accordance with the school's Low-Level Concerns Policy.

Where there is a concern that illegal activity has taken place, the Headteacher contacts the police.

All online safety incidents and the school's response are recorded by the DSL via CPOMS.

Responding to specific online safety concerns

Cyberbullying

Cyberbullying, against both students and staff, is not tolerated. Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur. Information about the school's full response to incidents of cyberbullying can be found in the Behaviour Management Policy.

Online sexual violence and sexual harassment between children (peer-on-peer abuse)

The school recognises that peer-on-peer abuse can take place online. Examples include the following:

- Non-consensual sharing of sexual images and videos

- Sexualised cyberbullying
- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSL via CPOMS who will investigate the matter in line with the Safeguarding and Child Protection Policy. Information about the school's full response to incidents of online peer-on-peer abuse can be found in the Safeguarding and Child Protection Policy.

Upskirting

Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

A "specified purpose" is namely:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear)
- To humiliate, distress or alarm the victim

"Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.

Upskirting is not tolerated by the school. Incidents of upskirting are reported to the DSL via CPOMS who will then decide on the next steps to take, which may include police involvement, in line with the Safeguarding and Child Protection Policy.

Youth produced sexual imagery (Nudes and semi-nudes, previously referred to as 'sexting')

Youth produced sexual imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal. This includes images that are digitally altered or wholly generated using artificial intelligence, including so called 'deepfakes' or 'deep nudes'. Staff must treat AI-generated or altered sexual imagery of a pupil with exactly the same seriousness and follow exactly the same immediate reporting to the DSL, as if it were a real photograph or video.

All concerns regarding sexting are reported to the DSL via CPOMS. Following a report of sexting, the following process is followed:

- The DSL holds an initial review meeting with appropriate school staff
- Subsequent interviews are held with the students involved, if appropriate
- Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the student at risk of harm
- At any point in the process if there is a concern a student has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately
- The interviews with staff, students and their parents are used to inform the action to be taken and the support to be implemented

When investigating a report, staff members do not view the youth produced sexual imagery unless there is a good and clear

reason to do so. If a staff member believes there is a good reason to view youth produced sexual imagery as part of an investigation, they discuss this with the headteacher first. The decision to view imagery is based on the professional judgement of the DSL and always complies with the Safeguarding and Child Protection Policy.

Any accidental or intentional viewing of youth produced sexual imagery that is undertaken as part of an investigation is recorded. If it is necessary to view the imagery, it will not be copied, printed or shared. Viewing and deleting imagery is carried out in line with the Behaviour Management Policy.

Online abuse and exploitation

Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it. The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment. All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL via CPOMS and dealt with in line with the Safeguarding and Child Protection Policy.

Online hate

The school does not tolerate online hate content directed towards or posted by members of the school community. Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved, e.g. Staff Code of Conduct, Anti-Bullying Policy.

Online radicalisation and extremism

The school's filtering system protects pupils and staff from viewing extremist content. Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the Safeguarding and Child Protection Policy and the Prevent Duty.

Remote learning

All remote learning is delivered in line with the school's Remote Learning Procedures. All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are only carried out where necessary
- Wear suitable clothing, this includes others in their household
- Be situated in a suitable area within the home with an appropriate background
- Use appropriate language, this includes others in their household
- Maintain the standard of behaviour expected in school
- Use the necessary equipment and computer programs as intended
- Not record, store, or distribute video material without permission

The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND, tutorials, pastoral support, sixth form choices etc. This will be decided and approved by a member of the Leadership Team.

Students not using devices or software as intended will be disciplined in line with the Behaviour Management Policy.
The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites
- Direct parents to useful resources to help them keep their children safe online

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Any safeguarding concerns arising during remote learning sessions must be reported immediately in line with the Safeguarding and Child Protection Policy.

Monitoring and review

The Governing Body, Headteacher and DSL review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is September 2027.