St Swithun's School Winchester

This policy applies to St Swithun's Senior School, St Swithun's Prep School and the Early Years Foundation Stage

Online Safety

Policy History	
Reviewed and updated	September 2026
Date of next review	September 2027

Reviewed by:

Deputy head (pastoral) and DSL Graham Yates Date: September 2026	Deputy Head and DSL Prep School Kate Grosscurth Date: September 2026
Head of IT Services Andy Healy Date: September 2026	Nominated Governor and School Council ratification Warwick Hill / Education Committee Date: October 2026

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place.

Contents

Scope of the Online Safety Policy 3
Process for monitoring the impact of the Online Safety Policy 4
Links with other policies and practices 4
Policy and leadership 6
Responsibilities 6
Policy 12
Online Safety Policy 12
Acceptable use 12
Reporting and responding 15
Online Safety Incident Flowchart 16
Responding to Student Actions 17
Responding to Staff Actions 18
Online Safety Education Programme 18
Staff 19
Parents/guardians/carers 20
Technology 21
Filtering 21
Monitoring 22
Technical Security 22
Social media 22
Digital and video images 26
Data Protection 27
Artificial Intelligence 27

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of the school to safeguard members of our entire school community online in accordance with statutory guidance and best practice. This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents, guardians and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site.

The policy also applies to online safety behaviour such as cyber-bullying, which may take place outside the school, but is linked to membership of the school. The school will deal with such behaviour within this policy and associated behaviour and discipline policies, and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

The School recognises that technological developments, including generative artificial intelligence (AI), present both opportunities and safeguarding risks. The School is committed to promoting a culture of safe, responsible and informed digital engagement and will ensure that pupils, staff and parents are supported to understand and respond appropriately to emerging online risks.

Process For Monitoring the Impact of the Online Safety Policy

The implementation of this policy will be monitored by the senior school deputy head (pastoral), Graham Yates, and DSL and the Prep school Deputy and DSL, Kate Grosscurth.

The school will monitor the impact of the policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited)
- internal monitoring data for network activity

In the future we plan to conduct:

- surveys/questionnaires of:
    - learners
    - parents and carers
    - staff

The School Council will receive a termly report from the DSLs on the implementation of the online safety policy which will include anonymous details of online safety incidents.

Should serious online safety incidents take place, these will be dealt with in line with the safeguarding policy and the anti-bullying policy.

Links with other policies and practices

This policy links with a number of other policies, including:

- Data protection policy
- Safeguarding and Child protection policy
- Staff Code of Conduct
- Staff IT Terms and Conditions
- Social media policy
- Behaviour policy (prep and senior)
- Anti-bullying policy (prep and senior)
- Searching, screening and confiscation policy
- Pupil IT Code of Conduct (prep and senior)
- Use of mobile phones policy – staff (prep school)
- Use of smart devices policy (prep school)
- Use of mobile phones policy (senior school)
- Nursery and Preschool online safety policy
- AI Policy

This policy is updated annually to reflect the latest KCSIE guidance and pays due regard to the following DfE guidance:

- Working Together to Safeguard Children (2026)
- Online Safety Act 2025
- Prevent Duty Guidance: for England and Wales (2015, updated 2023)
- The Prevent duty: Departmental advice for schools and childminders (2015, updated 2023)
- The use of social media for on-line radicalisation (July 2015)

- Meeting digital and technology standards in schools and colleges 2025: Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

- The Department has published Generative AI: product safety expectations - GOV.UK to support schools to use generative artificial intelligence safely, and explains how filtering and monitoring requirements apply to the use of generative AI in education.
- It has also produced a policy paper Generative artificial intelligence (AI) in education which considers the challenges and opportunities of AI for the education sector

Policy and leadership

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. All staff have a key role to play in feeding back on potential issues. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Headteachers

- The headteachers have a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the online safety Lead (senior school deputy head pastoral/DSL and prep school deputy head/DSL) .
- The headteachers and deputy head pastoral/prep school deputy head should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteachers are responsible for ensuring that the online safety lead, technical staff and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteachers/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteachers will receive regular monitoring reports from the online safety leads.

School Council

The School Council are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This is delegated to the Education Committee and the member of School Council with responsibility for online safety.

This review will be carried out in conjunction with the Online Safety Leads who will provide regular information about online safety incidents and monitoring reports. A member of the School Council will take on the responsibility of online safety (Warwick Hill) and this will include:

- regular meetings with the Online Safety Leads
- receiving regular (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy e.g. online safety education provision and staff training, is taking place as intended
- reporting to relevant School Council meetings
- ensuring that online safety forms part of the wider safeguarding framework;
- receiving assurance that effective filtering and monitoring systems are in place;
- ensuring an annual review of filtering and monitoring arrangements takes place;
- receiving regular safeguarding reports relating to online safety;
- ensuring appropriate resources and training are available.

Online Safety Lead

Graham Yates is the deputy head and Designated Safeguarding Lead (DSL) responsible for online safety for the senior school.
Kate Grosscurth is the deputy head and Designated Safeguarding Lead (DSL) responsible for online safety in the prep school.

The Online Safety Lead will:

- lead the Online Safety Group
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and the wider community
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to report those incidents immediately
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- identify sources of training and advice for staff, School Council, parents, carers or learners
- liaise with technical staff, pastoral staff and support staff, as relevant
- meet regularly with the online safety Member of Council to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant School Council meetings
- report regularly to headteacher/senior leadership team.

Designated Safeguarding Lead (DSL) and deputy DSLs

The designated safeguarding leads have lead responsibility for safeguarding and child protection including online safety and understanding the filtering and monitoring systems in place. They will:

- Ensure that ALL staff undergo online safety training, as part of their safeguarding training at induction and that this will include an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Ensure there is regular review and open communication where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible, but which cover areas of online safety (e.g. PSHE), and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused
- 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 (in harmony with policies for behaviour,

safeguarding, Prevent and others) and submit for review to School Council and the member of Council with responsibility for online safety.

- Ensure that online-safety education is embedded across the curriculum in line with the statutory PSHE guidance and beyond, in wider school life
- Promote an awareness of and commitment to online safety throughout the school community, including parents
- Communicate regularly with SLT and the safeguarding Member of Council to discuss current issues (anonymised), review incident logs and filtering/change control 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.

The DSL should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers/other children
- potential or actual incidents of grooming
- online bullying
- sharing nude and/or semi-nude images
- child sexual exploitation

Heads of department

Online safety education is delivered through PSHE and IT/Computing lessons. Relevant subject leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme. This will be provided through:

- a discrete programme
- PHSE and RSE programmes
- assemblies and pastoral programmes
- Resources available to pupils, parents and staff via the student wellbeing website and The Wellbeing Hub
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

PSHE Lead

The PSHE lead will:

- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE, relationships and sex education (RSE) and health education curriculum. This will include being taught 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. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives.

- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to identify where pupils need extra support or intervention through tests, written assignments or self-evaluations, to capture progress to complement the computing curriculum.
- Work closely with the DSL/online safety lead and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Computing Lead

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Teaching, boarding and support staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school's main safeguarding policy, the code of conduct/handbook and relevant parts of KCCSIE to support a whole-school safeguarding approach.

This includes reporting any concerns, no matter how small, to the designated safety lead, maintaining an awareness of current online safety issues and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond.

Staff should also be aware of the latest DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about over-blocking, gaps in provision or pupils bypassing protections.

Boarding staff should pay particular attention to **online tutors** hired by parents. They should share the Online Tutors – Keeping Children Safe poster at parentsafe.lgfl.net to remind parents of key safeguarding principles.

School staff are responsible for ensuring that, as well as adhering to the Staff Code of Conduct:

- they have an up-to-date awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding.
- they have read, understood, and signed the Staff IT Terms and Conditions

- they immediately report any suspected misuse or problem to the DSL or deputies for investigation/action, in line with the school safeguarding procedures
- ensure students understand and follow the Online Safety Policy and Pupil IT Code of Conduct
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use.
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Staff will receive regular online safety updates as part of safeguarding training. Training may include:

- emerging online risks;
- artificial intelligence;
- deepfakes and image-based abuse;
- cyber security awareness;
- filtering and monitoring processes;
- professional conduct online;
- online safeguarding reporting procedures.

Head of IT Services and the IT Services technical staff

The technical staff are responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Cybersecurity Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by relevant legislation
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant

- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring software/systems are implemented and regularly updated as agreed in school policies

Students

- are responsible for using the school digital technology systems in accordance with the relevant Pupil IT Code of Conduct and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand acceptable use and behaviour regarding the taking and or sharing of nude and semi-nude images, cyber-bullying, sharing of nudes and semi-nudes and grooming and other relevant online issues
- Should know where to access help and support when needed (e.g. through staff, online safety education, student wellbeing website and The Wellbeing Hub)

Parents, guardians and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- Publishing the school Online Safety Policy on the school website
- Providing them with a copy of the Pupil IT Code of Conduct
- Seeking their permissions concerning digital images, cloud services etc
- Publishing advice and guidance relating to online safety through the parent portal
- Providing access to guidance and resources through the parent pages of The Wellbeing Hub (senior school)

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school
- the use of their children's personal devices in the school

When a parent/guardian/carer supplies a student with a mobile device equipped with a mobile data SIM card, any filtering solution implemented by the school does not apply. They are therefore granting their child unfiltered/unmonitored internet access.
Prep school pupils are not permitted mobile phones/data enabled devices in school.

Community users and Guests

Community users and guests who access the guest Wi-Fi as part of the wider school provision must agree to an acceptable usage policy prior to gaining access to the school Wi-Fi.

Policy

Online Safety Policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels.
- is published to parents on the school portal.

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

This Online Safety Policy, the Staff IT Terms and Conditions, Pupil IT Code of Conduct define acceptable use at the school. These acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- splash screens
- communication with parents/carers
- teaching sessions as appropriate
- parent portal

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated images/sharing nudes/semi nudes – UKSIC Responding to and managing sexting incidents and Sharing nudes and semi-nudes					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to					X

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	X
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	

The school's web filtering policy can be viewed here for school staff:

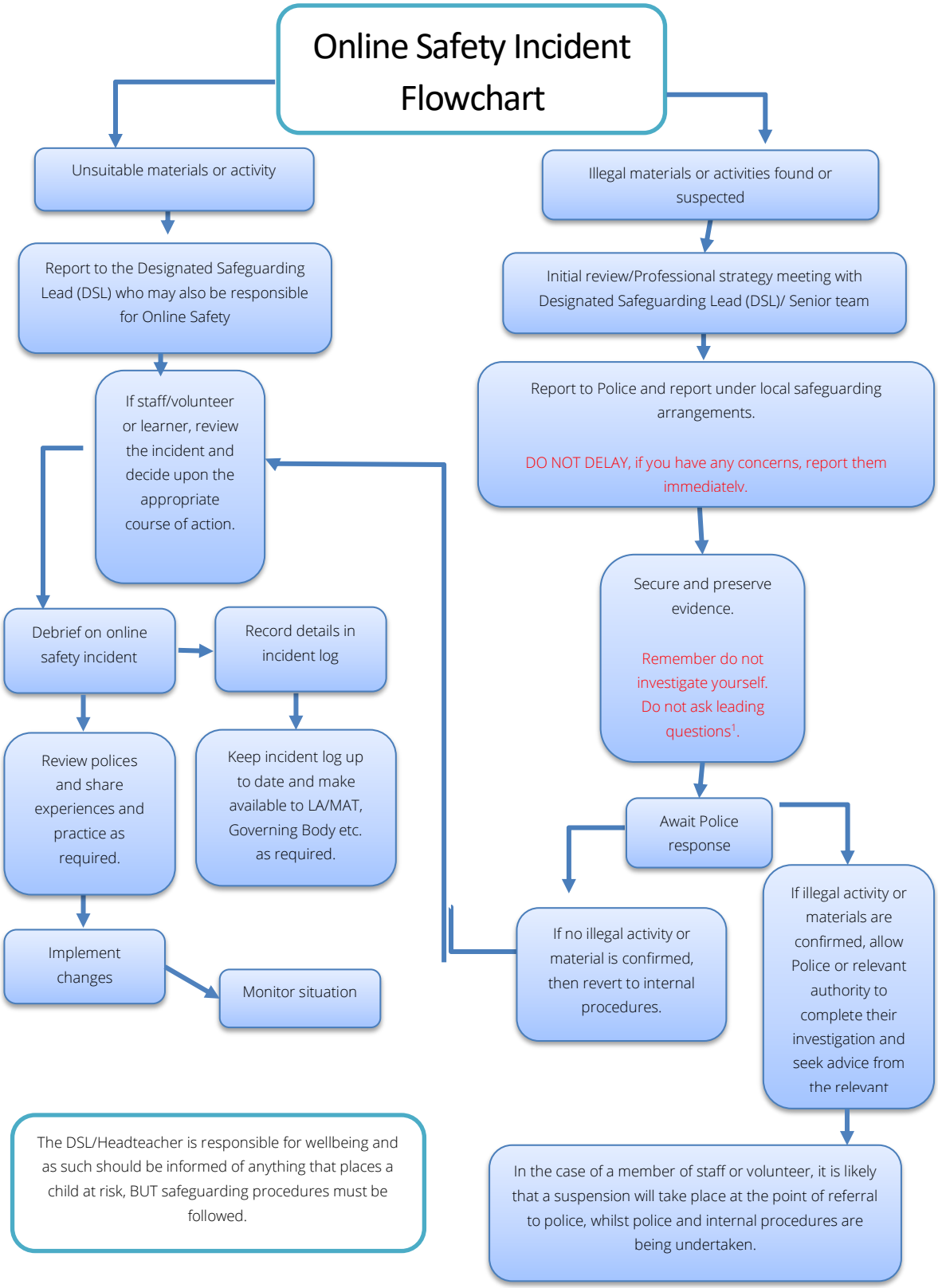
Web Filtering Policy

Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure that:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead(s)/Online Safety Leads and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors
- where there is no suspected illegal activity, devices may be checked in line with the searching, screening and confiscation policy,
- there are support strategies in place for those reporting or affected by an online safety incident
- incidents should be logged, both on CPOMS and on an online safety incident log held by the DSL
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues,
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions

The following flowchart can be used to guide the decision-making process for dealing with online safety incidents.



Online Safety Risks

The School recognises that safeguarding issues can manifest themselves via technology. Risks may include, but are not limited to:

- exposure to harmful, illegal or age-inappropriate content;
- misinformation, disinformation and conspiracy theories;
- cyberbullying;
- online grooming;
- child sexual exploitation and child criminal exploitation;
- coercive or controlling behaviour online;
- radicalisation and extremism;
- sharing or receiving indecent images;
- financial scams, fraud and online exploitation;
- misogynistic, discriminatory or hateful content;
- abuse facilitated by artificial intelligence (AI);
- deepfake and manipulated images or videos;
- image-based abuse, including the use of "nudification" applications;
- excessive or problematic online behaviours affecting health, wellbeing or education.

Pupils will be educated to understand the four broad categories of risk:

- Content
- Contact
- Conduct
- Commerce

As well as the emerging risks associated with generative AI technologies. See below.

Responding to Student Actions

The sorts of incidents that are most likely include:

- deliberately accessing or trying to access material that could be considered illegal
- Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords
- Corrupting or destroying the data of other users.
- Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.
- Unauthorised downloading or uploading of files or use of file sharing.
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic mate
- Deliberately accessing or trying to access offensive or pornographic material

- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act
- Unauthorised use of digital devices (including taking images)
- Unauthorised use of online service
- Actions which could bring the school into disrepute or breach the integrity or the ethos of the school
- Continued infringements of the above, following previous warnings or sanctions.

Depending on the nature and context of such incidents, responses may include:

- Issue of warning
- Education about appropriate / inappropriate actions
- Referral to tutor, head of department, head of year, deputy headteachers, headteacher
- Further sanction, in line with behaviour policy
- Removal of device and/or network access
- Referral to police
- Referral to children's services

Responding to Staff Actions

The sorts of incidents that will be investigated are most likely include:

- Deliberately accessing or trying to access material that could be considered illegal
- Deliberate actions to breach data protection or network security rules
- Deliberately accessing or trying to access offensive or pornographic material
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.
- Using proxy sites or other means to subvert the school's filtering system.
- Unauthorised downloading or uploading of files or file sharing
- Breaching copyright or licensing regulations.
- Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
- Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature
- Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers
- Inappropriate personal use of the digital technologies e.g. social media / personal e-mail
- Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school into disrepute or breach the integrity or the ethos of the school
- Failing to report incidents whether caused by deliberate or accidental actions
- Continued infringements of the above, following previous warnings or sanctions

Incidents will be investigated as directed by the head in whichever school the issue arises and, depending on the outcome of the investigation, appropriate action will be taken in line with our policies and statutory requirements. This may include disciplinary action and/or have contractual implications. If there is a concern that the issue relates to safeguarding, it will be dealt with according to the School's safeguarding policy.

Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum will be provided in the following ways:

- A planned online safety curriculum for all year groups. Lessons are matched to need, are age-related and build on prior learning.
- This will cover the four areas of risk within online safety:

- **Content** - age-inappropriate or unreliable content can be available to children. This includes being exposed to illegal, inappropriate or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **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,; See cyberbullying and grooming below.
- **Conduct** - children may be at risk because of their own behaviour, for example, by sharing too much information. Children need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet. It's easy to feel anonymous online and it's important that children are aware of who is able to view, and potentially share, the information that they may have posted. When using the internet, it's important to keep personal information safe and not share it with strangers. Conduct issues include making, sending and receiving explicit images including those generated using AI and online bullying; See sharing nudes and semi-nudes below. .
- **Commerce** - young people can be unaware of hidden costs and advertising in apps, games and websites. Risks such as online gambling, inappropriate advertising, phishing and or financial scams. See Gaming below. If we feel pupils, students or staff are at risk, we will report it to the Anti-Phishing Working Group (https://apwg.org/).

- It will also cover the risks of misinformation; disinformation; conspiracy theories; AI generated content; financial scams; online coercion and sextortion; deepfake technology and online misogyny; online sexual harassment and harmful influencer culture
- Digital competency is planned and effectively threaded through the appropriate elements in other curriculum areas
- To incorporate and make use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- The online safety curriculum will be regularly reviewed to reflect developments in technology and emerging safeguarding concerns.

Staff

At induction all new staff will cover the Staff Code of Conduct and will be required to sign the Staff IT Terms and Conditions. All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- all new staff will receive online safety training (including data protection training) as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom

management, professional conduct, online reputation and the need to model positive online behaviours.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- Online safety training will be delivered through staff meetings as required

Parents/guardians/carers

Parents, guardians and carers play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Some of the risks could be:

- unwanted contact
- grooming
- online bullying including sharing nudes and semi-nudes, including AI generated images or videos
- digital footprint
- accessing and generating inappropriate content
- misinformation, disinformation (including fake news), conspiracy theories
- generative artificial intelligence.

In light of this, the school will seek to provide information and awareness to parents and carers through communication, awareness-raising and engagement on online safety issues through signposting to relevant resources on the Parent Portal and signposting via SchoolPost.

Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

We pay due regard to the DfE guidance 'Meeting digital and technology standards in schools and colleges 2025'

The School uses appropriate filtering and monitoring systems to safeguard pupils whilst using the School's IT systems and network.

Filtering and monitoring arrangements will:

- be proportionate to the safeguarding risks faced by pupils;
- be regularly reviewed;
- support the identification of safeguarding concerns;
- be understood by safeguarding, leadership and technical staff.

Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

Filtering

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined both in the UK Safer Internet Centre Appropriate filtering document and the DfE's 'Meeting digital and technology standards in schools and colleges 2025'
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes
- the school has provided enhanced/differentiated user-level filtering, allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/students/guests, etc.
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.

- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.
- a member of Internet Watch Foundation (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal content including child sexual abuse material (CSAM)

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment. These include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where technically and proportionately possible, the school applies filtering and monitoring protections to school-owned devices regardless of location, helping to safeguard students both on and off site.
- The school uses a combination of automated and human-reviewed third-party monitoring services to identify potential safety concerns. Where serious or urgent risks to a student's welfare are identified, alerts are escalated to the DSL via phone call to allow a prompt and appropriate safeguarding response.

The DSL, relevant safeguarding staff and IT personnel will work together to ensure that alerts generated through monitoring systems are reviewed promptly and acted upon where appropriate.

The effectiveness of filtering and monitoring arrangements will be formally reviewed at least annually and outcomes will be reported to governors.

Technical Security

See IT Technical and Cyber Security Policy

Specific online safety safeguarding issues

Cyberbullying

Central to the school's anti-bullying policy is the principle that '*bullying is always unacceptable'* and that '*all students have a right not to be bullied*'. The school also recognises that it must take note of bullying perpetrated outside school which spills over into the school; therefore, once aware we will respond to any cyber-bullying we become aware of carried out by students when they are away from the site.

Cyber-bullying is defined as 'an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself.'

By cyber-bullying, we mean bullying by electronic media:

- Bullying by texts or messages or calls on mobile 'phones
- The use of mobile 'phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in on-line forums

Cyber-bullying may be at a level where it is criminal in character. It is unlawful to disseminate defamatory information in any media including internet sites.

Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.

The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

If we become aware of any incidents of cyberbullying, we will need to consider each case individually as to any criminal act that may have been committed. The school will pass on information to the police if it feels that it is appropriate or is required to do so.

Cybercrime

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

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

- denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Additional advice can be found at: *Cyber Choices, 'NPCC- When to call the Police'* and *National Cyber Security Centre - NCSC.GOV.UK*

Sharing nudes or semi-nudes (previously known as sexting)

The sharing of nude or semi-nude pictures or videos through mobile phones and/or the internet (sometimes referred to as sexting) is always a safeguarding matter. It includes underwear shots, sexual poses and explicit text messaging. Increasingly, this definition also encompasses the creation, possession or sharing of sexualised, nude or semi-nude images generated or manipulated using artificial intelligence (AI), including the use of "nudification" apps, deepfakes and other AI tools that can alter or create images of a person without their consent.

While the sharing of nudes and semi-nudes can take place within a consensual relationship between two young people, the use of sexual images in revenge following a relationship breakdown is becoming more commonplace. The sharing of nudes and semi-nudes can also be used as a form of sexual exploitation and may take place between strangers. In addition, AI technology can be used to facilitate bullying, harassment, coercion, exploitation and child-on-child abuse through the creation or sharing of manipulated, sexualised or degrading images.

As the average age of first smartphone or camera-enabled tablet ownership continues to fall, sharing nudes and semi-nudes, including AI-generated or AI-manipulated imagery, is an issue that requires awareness raising across all age groups.

The school will use age-appropriate educational materials to raise awareness, promote online safety, develop digital resilience and help pupils understand issues relating to consent, privacy, peer pressure and the responsible use of technology, including AI. Parents should be aware that they can come to the school for advice and support.

In cases where nudes or semi-nudes have been shared, we follow guidance given to schools and colleges by the DfE: Sharing nudes and semi-nudes: advice for education settings working with children and young people. This is broadly as follows:

Initial response

- the incident should be referred to the DSL (or equivalent) as soon as possible
- the DSL (or equivalent) should hold an initial review meeting with appropriate staff. This may include the staff member(s) who heard the disclosure and the safeguarding or leadership team who deal with safeguarding concerns
- there should be subsequent interviews with the children or young people involved (if appropriate)
- parents and carers should be informed at an early stage and involved in the process in order to best support the child or young person unless there is good reason to believe that involving them would put the child or young person at risk of harm
- a referral should be made to children's social care and/or the police immediately if there is a concern that a child or young person has been harmed or is at risk of immediate harm at any point in the process

Initial review meeting

This should consider the initial evidence and aim to establish:

- whether there is an immediate risk to any child or young person
- if a referral should be made to the police and/or children's social care
- if it is necessary to view the image(s) in order to safeguard the child or young person – in most cases, images or videos should not be viewed - for further guidance on when an image may need to be viewed see below
- what further information is required to decide on the best response
- whether the image(s) has been shared widely and via what services and/or platforms. This may be unknown
- whether immediate action should be taken to delete or remove images or videos from devices or online services
- any relevant facts about the children or young people involved which would influence risk assessment
- if there is a need to contact another education, setting or individual
- whether to contact parents or carers of the children or young people involved - in most cases they should be involved

The DSL may refer to the harmful sexual behaviours guidance in the Safeguarding & Child protection policy to help assess the behaviours of any child involved to identify any immediate risks. An immediate referral to police and/or children's social care through the MASH should be made if:

1. The incident involves an adult. Where an adult poses as a child to groom or exploit a child or young person, the incident may first present as a child-on-child incident.
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs).
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any child or young person in the images or videos is under 13

5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming.

The decision to respond to the incident without involving the police or children's social care should only be made in cases where the DSL (or equivalent) is confident that they have enough information to assess the risks to any child or young person involved and the risks can be managed within the education setting's pastoral support and disciplinary framework and, if appropriate, their local network of support.

The decision should be made by the DSL (or equivalent) with input from the headteacher/or manager and leadership team and input from other members of staff if appropriate. The decision should be made and recorded in line with the education setting's safeguarding or child protection procedures and should be based on consideration of the best interests of any child or young person involved. This should take into account proportionality as well as the welfare and protection of any child or young person. The decision should be reviewed throughout the process of responding to the incident.

If doubts remain after following child protection procedures, local safeguarding arrangements should be followed.

Assessing the risks once the images have been shared

When assessing the risks and determining whether a referral is needed, the following should be also considered:

- Why was the nude or semi-nude shared? Was it consensual or was the child or young person put under pressure or coerced?
- Has the nude or semi-nude been shared beyond its intended recipient? Was it shared without the consent of the child or young person who produced the image?
- Has the nude or semi-nude been shared on social media or anywhere else online? If so, what steps have been taken to contain the spread?
- How old are any of the children or young people involved?
- Did the child or young person send the nude or semi-nude to more than one person?
- Do you have any concerns about the child or young person's vulnerability?
- Are there additional concerns if the parents or carers are informed?

Searching devices, viewing and deleting nudes and semi-nudes

The School's 'Search and Confiscation' policy can be found here.

Staff and parents or carers must not intentionally view any nudes and semi-nudes unless there is good and clear reason to do so as outlined below. Wherever possible, responses to incidents should be based on what DSLs (or equivalents) have been told about the content of the imagery.

The decision to view any imagery should be based on the professional judgement of the DSL (or equivalent) and should always comply with the child protection policy and procedures of the

education setting. Imagery should never be viewed if the act of viewing will cause significant distress or harm to any child or young person involved.

If a decision is made to view imagery, the DSL (or equivalent) would need to be satisfied that viewing:

- Is the only way to make a decision about whether to involve other agencies because it is not possible to establish the facts from any child or young person involved
- is necessary to report it to a website, app or suitable reporting agency (such as the IWF) to have it taken down, or to support the child or young person or parent or carer in making a report
- is unavoidable because a child or young person has presented it directly to a staff member or nudes or semi-nudes have been found on an education setting's device or network

If it is necessary to view the imagery then the DSL (or equivalent) should:

- never copy, print, share, store, save or forward them; this is illegal.
- discuss the decision with the headteacher
- make sure viewing is undertaken by the DSL (or equivalent) or another member of the safeguarding team with delegated authority from the headteacher or a member of the senior leadership team
- make sure viewing takes place with another member of staff present in the room, ideally the headteacher or a member of the senior leadership team. This staff member does not need to view the images.
- wherever possible, make sure viewing takes place on the premises of the education setting, ideally in the headteacher or a member of the senior leadership team's office
- make sure wherever possible that they are viewed by a staff member **of the same sex as the child** or young person in the images
- record how and why the decision was made to view the imagery in the safeguarding or child protection records, including who was present, why the nudes or semi-nudes were viewed and any subsequent actions. Ensure this is signed and dated and meets any appropriate wider standards e.g. such as those set out in statutory safeguarding guidance and local authority policies and procedures.
- if any devices need to be taken and passed onto the police, the device(s) should be confiscated and the police should be called. The device should be disconnected from Wi-Fi and data, and turned off immediately to avoid imagery being removed from the device remotely through a cloud storage service. The device should be placed in a secure place, for example in a locked cupboard or safe until the police are able to come and collect it.

Deletion of imagery (from devices and social media)

If the school has decided that involving other agencies is not necessary, consideration should be given to deleting the images. It is recommended that students are asked to delete the images themselves and confirm they have done so. They should be given a deadline for deletion across all devices, online storage, or social media sites. They should be reminded that possession of nudes and semi-nudes is illegal. They should be informed that if they refuse or it is later discovered they did not delete the imagery, they are continuing to commit a criminal offence and the police may become involved.

Any decision to search a child or young person's device and delete imagery should be based on the professional judgement of the DSL (or equivalent) and should always comply with our safeguarding and child protection policy. All decisions need to be recorded, including times, dates and reasons for decisions made and logged in the safeguarding records. Parents and carers should also be informed unless this presents a further risk to any child or the young person.

All incidents relating to nudes and semi-nudes being shared need to be recorded.

Gaming

Online gaming is an activity in which the majority of children and many adults get involved. The school will raise awareness:

- By sharing relevant information with parents through social media, bulletins, newsletters etc
- By talking to parents and carers about the games their children play and help them identify whether they are appropriate
- By supporting parents in identifying the most effective way to safeguard their children by using parental controls and child safety mode
- By talking to parents about setting boundaries and time limits when games are played
- By highlighting relevant resources.

Online reputation

Online reputation is the opinion others get of a person when they encounter them on-line. It is formed by posts, photos that have been uploaded and comments made by others on people's profiles. It is important that children and staff are aware that anything that is posted could influence their future professional reputation. The majority of organisations and work establishments now check digital footprints before considering applications for positions or places on courses.

Grooming

On-line grooming is the process by which one person with an inappropriate sexual interest in children will approach a child on-line, with the intention of developing a relationship with that child, to be able to meet them in person and intentionally cause harm.

The school will build awareness amongst children and parents about ensuring that the child:

- Only has friends on-line that they know in real life
- Is aware that if they communicate with somebody that they have met on-line, that relationship should stay on-line.

That the school will support parents to:

- Have regular conversations with their children about on-line activity and how to stay safe on-line

The school will raise awareness by:

- Disseminating relevant information to parents via Schoolpost and the Parent Portal
- Include awareness around grooming as part of their curriculum
- Identifying with parents and children how they can be safeguarded against grooming.

Violence against women and girls

The School recognises the increasing influence of online platforms in shaping attitudes and behaviours.

The School will actively challenge:

- misogyny;
- sexual harassment;
- image-based abuse;
- harmful gender stereotypes;
- online communities promoting violence against women and girls;
- discriminatory and abusive online behaviour.

Concerns will be addressed through safeguarding procedures, behaviour management, RSHE education and pastoral support.

Social media

See Social Media policy

Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- staff must be aware of those learners whose images must not be taken/published. All images should only be taken on school devices.
- The personal devices of staff should not be used for any such purposes as outlined in the staff code of conduct
- staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs

- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. This is usually provided by the permission form on first admission to the school.
- images will be securely stored in line with the school retention policy

Data Protection

See Data Protection policy

Artificial Intelligence

The School recognises that artificial intelligence technology is developing rapidly and may create safeguarding concerns.

Risks may include:

- AI-generated misinformation and disinformation;
- deepfake images and videos;
- AI-generated indecent imagery;
- grooming or exploitation using AI-enabled tools;
- impersonation and fraud;
- academic malpractice;
- misuse of AI chatbots and image-generation platforms.

Pupils will receive age-appropriate education to help them:

- identify AI-generated content;
- critically evaluate information encountered online;
- understand how AI may be used maliciously;
- report concerns regarding AI-enabled abuse or exploitation.

Staff will receive training on emerging AI risks and the School's expectations regarding the safe and ethical use of AI technologies.

Artificial Intelligence (AI) tools are becoming increasingly prevalent and have a wide-ranging impact on education. There are obvious concerns and nervousness regarding use of AI including data privacy, security, academic dishonesty and exam integrity. Equally, Large Language models (LLM) such as ChatGPT can be a powerful aid for research and assignments. These same tools can potentially generate entire pieces of work and the challenge for staff is to identify such submissions as plagiarism. Students should not rely on AI to complete their work but, instead, could use it as a personal tutor, when permitted by the teacher. They should also be aware that LLMs are not fool-proof and should cross-check AI responses for accuracy. Correct use of AI is taught as part of PSHE and Computing lessons. Misuse of AI will be treated in line with the school's behaviour policy.

Artificial Intelligence Child Sexual Abuse Material (CSAM)

This is one of the rapidly escalating safeguarding issues for young people. We need to be aware that any AI CSAM is illegal and should be reported immediately. Young people may create AI-CSAM of peers thinking its 'just a joke' or 'banter'. Support can be found through:

Shorespace - an organisation that helps young people get help and support on anything related to sexual relationships and their, or others, behaviour

Report Remove - a way to help young people to confidentially report sexual images and videos of themselves and remove them from the internet.