E-Safety, Mobile Phone & ICT Policy

Approved	22 April 2026
Review cycle:	Annual: April 2027 (or more regularly in the light of any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place)
Party responsible:	E-safety Co-ordinator, Headteacher and the Student Committee
Linked policies:	Child Protection & Safeguarding, Behaviour & Exclusions, Child-on Child Abuse, Complaints, Preventing & Tackling Bullying, Artificial Intelligence, Staff Disciplinary procedures, Data Protection and Privacy Notices

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Implement clear guidelines on the use of mobile and smart technology on school grounds to minimise distractions and safeguard pupils from online risks during the school day
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Work collaboratively with parents, carers, and external agencies to reinforce safe online behaviours and ensure a consistent message inside and outside of school.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk (in line with KCSIE 2025, paragraph 135)

- **Content** being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, deepfake or AI-generated harmful material, including manipulated media designed to deceive or defraud, and misinformation, disinformation (including fake news) and conspiracy theories

- **Contact** being subjected to harmful online interaction with other users, such as 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 and exploitation via emerging digital platforms, including AI-driven chatbots or social media manipulation
- **Conduct** personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce risks** such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education (KCSIE) 2025, and its advice for schools on:

- Teaching online safety in schools (2023)
- Cyber-bullying: advice for headteachers and school staff
- Relationships, Sex and Health Education (RSHE) – note: revised statutory RSHE guidance is expected; this policy will be updated to reflect it once published, as signposted in KCSIE 2025
- Searching, screening and confiscation (2022)
- The use of mobile phones in schools (Feb 2026)
- Generative AI: product safety expectations (DfE) – (Jan 2026)
- Plan Technology for Your School service (DfE, Updated 2026) – for self-assessment against filtering and monitoring standards

It also refers to the DfE's guidance on protecting children from radicalisation, including the Prevent Duty Guidance (2023 update).

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy also aligns with the Online Safety Act 2023, which strengthens protections against harmful digital content. It takes into account data protection legislation, including the Data Protection Act 2018 and UK GDPR, ensuring responsible handling of pupil data in online contexts. Staff, governors and trustees are directed to the DfE Data Protection Guidance for Schools to understand their data protection obligations, including in relation to filtering, monitoring and AI systems.

The policy also takes into account the National Curriculum computing programmes of study and reflects the statutory status of Working Together to Improve School Attendance (2024).

3. Roles and responsibilities

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The governor who oversees online safety is Tim Marcus

- The online safety governor should liaise regularly with the DSL and ensure staff training is effective.
- Governors must satisfy themselves that the school has sufficient and appropriate filtering and monitoring in place, using the DfE's Plan Technology for Your School self-assessment service to evidence an annual review

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Receive safeguarding training, including online safety, as part of their governor induction and at regular intervals

The governing board is responsible for ensuring compliance with statutory safeguarding duties under KCSIE 2025.They will provide strategic oversight of online safety, ensuring appropriate policies, procedures, and training are in place

3.2 The Headteacher

The Headteacher is responsible for embedding a whole-school approach to online safety, ensuring staff, pupils, and parents are aware of the school's expectations and procedures.

- The Headteacher will ensure that safeguarding education, including online safety, is tailored where necessary to meet the needs of vulnerable children, victims of abuse and pupils with SEND. Recognising that a 'one size fits all' approach may not be suitable for all children, the Headteacher will promote a personalised and/or contextualised approach to ensure it is effective and accessible for all learners
- The Headteacher will ensure that the school's approach to online safety encompasses emerging risks including generative AI, deepfakes, misinformation and conspiracy theories

3.3 The Designated Safeguarding Lead

Details of the school's DSL and deputies are set out in our Child Protection and Safeguarding policy as well as relevant job descriptions.

The DSL holds overall responsibility for leading online safety within school. In particular, the DSL will:

- Support the Headteacher in ensuring all staff understand this policy and apply it consistently throughout the school

- Work collaboratively with the headteacher, IT Manager, Business Manager and other staff as necessary, to address any online safety concerns or incidents
- Manage all online safety issues and incidents in line with the school Child Protection Policy
- Ensure that any online safety incidents are logged on MyConcern and addressed appropriately in line with this policy
- Monitor and address cyberbullying incidents, ensuring they are logged and managed appropriately in line with the school's Behaviour Policy
- Lead on staff training and updates related to online safety, ensuring staff are equipped with the necessary knowledge and skills, including in relation to misinformation, disinformation and conspiracy theories
- Liaise with external agencies and external services if necessary to support online safety measures
- Provide regular reports on online safety treads, incidents and developments in school, to the headteacher and/or governing board
- Ensure the school's annual risk assessment considers evolving online harms including AI-generated content, deepfakes, and emerging platforms

This list is not intended to be exhaustive and may evolve in response to emerging online risks and safeguarding priorities.

3.4 The Business Manager

The Business Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, in line with DfE's 'Filtering and Monitoring Standards (updated 2024), which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring cyber security resilience, including tested backup and restore procedures, multi-factor authentication (MFA) for administrators, secure Wi-Fi and switching configurations, and regular patching of systems
- Using the DfE's Plan Technology for Your School self-assessment service annually to assess the school against filtering and monitoring standards and produce evidence of compliance for the governing board
- IT staff must complete annual training on the school's filtering and monitoring systems, ensuring they are able to identify and respond to potential risks effectively
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Incidents of cyberbullying or online harassment will be dealt with in line with the school's behaviour policy. The Business Manager will work with the DSL to ensure that appropriate sanctions are applied and that support is provided to both the victim and the perpetrator.

Any incidents involving safeguarding concerns, including online bullying, inappropriate content, or harmful contact, must be immediately escalated to the DSL via MyConcern. Incidents involving concerns about radicalisation, extremism, or exposure to terrorist material must be reported to the DSL without delay. The DSL will follow the school's Prevent Duty procedures, which may include making a referral to the local Channel Panel or contacting the police if there is an immediate risk. The Business Manager will support the DSL by ensuring that all relevant IT data (e.g., browsing history or login attempts) is preserved and made available for investigation.

- Ensuring the school's Data Protection Officer (DPO) is involved in decisions relating to filtering and monitoring systems, AI tools, and any data protection impact assessments (DPIAs) relating to new technologies
- Ensuring they review the DfE filtering and monitoring standards and make sure the school is compliant with the requirements to meet these duties through discussions with IT staff and service providers.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Completing regular e-safety training (annually), as directed, to stay updated on emerging risks and safeguarding practices
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Monitor ICT activity in lessons, extra-curricular and extended Academy activities
- Logging online safety incidents and concerns via the MyConcern and Working with the DSL to ensure that any dealt with appropriately in line with this policy
- Identifying and reporting concerns related to radicalisation or extremist content online in line with The Prevent Duty
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Modelling safe and responsible online behaviour for students, and read, understand and sign off the Staff Acceptable Use Agreement (Appendix 2)

- All staff working directly with children must read at least Part 1 of KCSIE 2025. Those who do not work directly with children should read Annex A of KCSIE 2025

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy. E-safety concerns can be reported to office@theswanageschool.co.uk
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- UK Safer Internet Centre: www.saferinternet.org.uk
- Internet Matters: www.internetmatters.org
- CEOP / Think You Know: www.thinkuknow.co.uk
- Childnet International: www.childnet.com
- NSPCC: www.nspcc.org.uk/onlinesafety
- Disrespect Nobody: www.disrespectnobody.co.uk

3.7 Visitors and members of the community

- Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it
- When appropriate, visitors and community members will be required to read and agree to the school's Acceptable Use Policy (Appendix 2) before accessing ICT systems
- Visitors and community members will only be granted access to the school's ICT systems or internet under supervision, unless explicitly authorised by a senior leader or the Business Manager
- Visitors and community members must report any concerns about online safety or inappropriate use of the school's ICT systems to a member of staff immediately
- They are expected to comply with the school's safeguarding procedures, including the Prevent Duty
- If the school provides a guest Wi-Fi network, visitors will only be granted access to this network, which will have appropriate filtering and monitoring in place

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum, in line with the National Curriculum computing programmes of study, statutory guidance on Relationships Education, Relationships and Sex Education (RSE), and Health Education. The school recognises that online safety education is essential to equip pupils with the knowledge and skills to navigate the digital world safely and responsibly.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- Develop critical thinking skills to evaluate the reliability of online information and identify misinformation, disinformation, fake news and conspiracy theories

- Understand the risks associated with social media, gaming, and online communication platforms, including the potential for grooming, exploitation, and cyberbullying

Pupils in **Key Stage 4** will be taught:

- How changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns, including cyberbullying, harassment and exposure to harmful content
- The legal and ethical implications of online behaviour, including the consequences of sharing indecent images, engaging in hate speech, or participating in illegal activities onlineHow to recognise, critically evaluate and challenge misinformation, disinformation and conspiracy theories encountered online
- Responsible use of generative AI tools, including understanding the risks of AI-generated content, deepfakes and data privacy implications

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online and offline
- About online risks, including that any material provided to another person has the potential to be shared, copied or used without consent; the difficulty of removing potentially compromising material placed online; not to provide material to others that they would not want shared further; and not to share personal material which is sent to them
- The importance of not sharing personal material or content that could harm themselves or others
- The risks and opportunities associated with emerging technologies, such as artificial intelligence (AI), virtual reality (VR), and augmented reality (AR), and how to use these tools responsibly
- How to identify and challenge misinformation, disinformation (including fake news) and conspiracy theories encountered online
- How to respond to harmful content and behaviour, including: what to do and where to get support; the impact of viewing harmful content including self-harm, extremist material and pornography; and that pornography presents a distorted picture of sexual behaviours
- That sharing and viewing indecent images of children (including those created by children or by AI) is a criminal offence which carries severe penalties including imprisonment
- How information and data is generated, collected, shared and used online, including risks of data breaches, identity theft and exploitation
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if affected
- The importance of consent in all online interactions, including how to actively communicate and recognise consent, how consent can be withdrawn, and the legal and ethical implications of sharing intimate images without consent

Online safety will be reinforced across the curriculum. Where necessary, teaching about safeguarding, including online safety, will be adapted to meet the needs of vulnerable children, victims of abuse and pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety through letters, newsletters, other communications home, and the school website, including updates on emerging risks (e.g., social media, gaming, AI tools, misinformation and deepfakes). This policy will also be shared with parents.

Online safety will also be covered during parents' evenings, with resources provided from organisations like NSPCC and CEOP. Parents are encouraged to discuss online safety with their children and monitor their online activity. Any queries or concerns in relation to online safety should be raised in the first instance with the headteacher and/or the DSL.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, or through digital devices, such as through social networking sites, messaging apps, gaming sites or via text messages. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where there is an imbalance of power. Cyber-bullying can include:

- Sending abusive or threatening messages.
- Sharing private or embarrassing information without consent.
- Excluding someone from online groups or activities.
- Creating fake profiles to harass or impersonate others.
- Using AI tools to generate fake or manipulated images/content to target individuals (deepfakes)

(See also the school Behaviour Policy.)

6.2 Preventing and addressing cyber-bullying

To prevent and address cyber-bullying, the school will ensure that pupils understand what cyberbullying is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. The school will teach pupils about the legal consequences of cyber bullying, including the misuse of social media and sharing intimate images. Crew Leaders will discuss cyber-bullying with their Crews. We will provide clear, accessible ways for pupils to report cyber-bullying, including anonymous reporting options, and ensure pupils know they can speak to a trusted adult, such as their Crew Leader, a teacher, or the DSL.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying, including personal, social, health and economic (PSHE) education and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) will receive regular training on cyber-bullying, its impact and how to support pupils, as part of safeguarding training (see section 11).

The school will share information with parents about cyber-bullying so that they are aware and can recognise the signs, how to report it and how they can support children who may be affected, providing resources from organisations such as CEOP, NSPCC and Childnet.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been shared among pupils, the school will take reasonable steps to contain the incident. The DSL will assess whether the

incident involves illegal material (e.g., indecent images, hate speech, AI-generated content used to harm, or threats) and, if necessary, report it to the police or other relevant authorities.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, tablets and other devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation, and the UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are required to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1-2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

The school will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

The school uses filtering and monitoring systems that comply with the DfE's Filtering and Monitoring Standards to block access to inappropriate or harmful content. The school will use the DfE's Plan Technology for Your School self-assessment service annually to evidence compliance with these standards.

Users must respect the privacy of others and comply with the school's Data Protection Policy and UK GDPR. This includes not sharing personal information or images without consent. The school's Data Protection Officer (DPO) is involved in the governance of filtering, monitoring and AI systems.

More information is set out in the Acceptable Use Agreements in Appendices 1 and 2.

7.1 Generative Artificial Intelligence (AI)

The school recognises that generative AI tools (such as AI chatbots and AI image generators) present both educational opportunities and safeguarding risks. The school will:

- Ensure that any generative AI tools used in school meet the DfE's product safety expectations for AI in education
- Assess risks associated with AI tools through Data Protection Impact Assessments (DPIAs) in consultation with the school's DPO before adoption
- Educate pupils about responsible AI use, including understanding how AI-generated content is created, the potential for deepfakes and misinformation, and the data privacy implications of using AI tools
- Train staff on the appropriate and responsible use of AI tools in an educational setting, and on the risks of AI-generated content including deepfakes and disinformation
- Ensure filtering and monitoring systems are reviewed for their effectiveness in identifying AI-generated harmful content
- Not permit pupils to use AI tools to generate content that could be harmful, offensive, or used to harass others

Staff and pupils must not input personal data about pupils, staff or other individuals into publicly available AI tools without appropriate authorisation and a completed DPIA.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but their use is strictly regulated to minimise disruption and to ensure a safe learning environment. The following rules apply:

During the school day:

- Mobile devices must not be used during the school day unless explicit permission is granted by a member of staff for educational purposes or in exceptional circumstances.
- Devices should be switched off and stored securely

Before and after school:

- Mobile devices may only be used before or after school, or during clubs and activities, if explicitly permitted by the supervising adult.
- Any use must be in line with the school's acceptable use agreement (see Appendix 1).

Consequences for Misuse:

- Any breach of the acceptable use agreement, including unauthorised use of mobile devices, will be treated as a behavioural issue and addressed in line with the school behaviour policy.
- This may result in the confiscation of the device, which will be returned at the end of the school day or to a parent/carer, depending on the severity of the breach.

Safeguarding Considerations:

- The school recognises that mobile devices can pose safeguarding risks, such as cyber-bullying, inappropriate content, or unauthorised recording. and access to AI tools. Staff will remain vigilant and take appropriate action if concerns arise. Staff will remain vigilant and take appropriate action if concerns arise.
- Pupils will be educated about the responsible use of mobile devices as part of the school's e-safety curriculum.

Unauthorised Photos or Recordings:

- Pupils, staff, visitors, and parents/carers are not permitted to take photos or recordings of students in school uniform on school premises without prior consent from the school.
- This includes photos or videos taken on mobile devices, cameras, or other recording equipment.
- Any unauthorised photography or recording will be treated as a breach of the school's acceptable use agreement and addressed in line with the school behaviour policy.
- Devices used to take unauthorised photos or recordings may be confiscated, and the material deleted. In serious cases, the incident may be reported to the DSL or, if necessary, the police.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Enabling encryption on the device to protect data if lost or stolen.
- Setting devices to lock automatically t inactive for a short period of time
- Devices much not be shared among family or friends
- Installing, and regularly updating anti-virus and anti-malware software
- Keeping operating systems and applications up to date with the latest updates
- Using multi-factor authentication (MFA) where available for school systems accessed remotely

Staff must comply with the school's acceptable use policy (Appendix 2) at all times. Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek immediate advice from the Business Manager or IT Manager.

10. Staff Using Personal Devices for school-related work

Staff should avoid storing school information about individuals on a personal device.

Any school data should not be stored on a personal device for longer than needed, compliant with all data protection requirements.

Staff should ensure the personal device is locked when unattended and has password and/ or biometric (eg Touch ID or facial recognition) protection.

If the personal device is lost or stolen, this must be reported to the school immediately.

It is the responsibility of staff that school data on a personal device is not accessible by other people.

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, the school will follow the procedures set out in the behaviour policy and ICT and internet acceptable use policy. The action taken will be proportionate and depend on the individual circumstances, nature and seriousness of the specific incident.

Where a staff member misuses the school's ICT systems, internet or a personal device in a way that constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents involve illegal activity, online harassment, extremist content, AI-generated harmful material, or the spread of dangerous misinformation, and whether these should be reported to the police or other relevant authorities.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying, peer-on-peer abuse, the risks of online radicalisation, and the safeguarding risks associated with generative AI and disinformation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training. Regular updates will also be provided through emails, e-bulletins and staff meetings.

By way of this training, all staff will be made aware that:

- Technology plays a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Misinformation, disinformation (including fake news) and conspiracy theories are recognised online safeguarding harms that can radicalise or harm children

  KCSIE 2025 (para 135) explicitly lists misinformation, disinformation and conspiracy theories as safeguarding harms. Staff training must address these.
- Children can abuse their peers online through abusive, harassing, and misogynistic messages; non-consensual sharing of indecent images and/or videos, especially around chat groups; and sharing abusive content including images and pornography to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence often contain an online element

- The safeguarding risks associated with AI-generated content including deepfakes, AI chatbots and manipulation through digital platforms

Training will also help staff:

- Develop awareness to identify signs and symptoms of online abuse
- Equip pupils with the skills to recognise online dangers and make informed, healthy choices
- Understand how to identify and respond to disinformation, misinformation and conspiracy theories in an educational context

The DSL and deputies will undertake child protection and safeguarding training, including online safety, at least every 2 years. They will also update their knowledge and skills on online safety annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates on online safety, if applicable.

More information about safeguarding training is set out in our Safeguarding Children & Child Protection policy.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety via the MyConcern reporting system. This ensures a consistent and secure method of recording and tracking incidents.

- This policy will be reviewed annually by the DSL to ensure it remains up to date and effective. The reviewed policy will be shared with the governing body for approval and oversight
- The annual review will be supported by a comprehensive annual risk assessment that considers and reflects the evolving risks pupils face online. including changes in technology, AI, emerging online harms, and the school's current safeguarding practices
- The risk assessment will inform updates to the policy and help the school proactively address new challenges.

Appendix 1: KS3 and KS4 Acceptable Use Agreement (Pupils and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil: _____

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a member of staff is present, or with a staff member's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a member of staff (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it
- Think critically about information I find online, and report anything I think might be false, misleading or harmful (including fake news and conspiracy theories) to a member of staff

I will not:

- Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a member of staff
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Use AI tools to generate harmful, offensive or misleading content, or to impersonate others

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a staff member's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil): _____ Date: _____

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer): _____ Date: _____

Appendix 2: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

_____

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms for personal use
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with a member of staff first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school
- Input personal data about pupils, staff or other individuals into publicly available AI tools without appropriate authorisation and a completed Data Protection Impact Assessment (DPIA)

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will use multi-factor authentication (MFA) where available for school systems.

I will let the Designated Safeguarding Lead (DSL), Business Manager and Head Teacher know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed (staff /governor/volunteer/visitor): _____ Date: _____

Links to Other Organisations and Resources

- UK Safer Internet Centre: www.saferinternet.org.uk
- South West Grid for Learning: www.swgfl.org.uk
- Childnet: www.childnet.com
- Internet Watch Foundation: www.iwf.org.uk
- CEOP: www.ceop.police.uk
- Think U Know: www.thinkuknow.co.uk
- NSPCC Online Safety: www.nspcc.org.uk/onlinesafety
- DfE Plan Technology for Your School (filtering & monitoring self-assessment): www.gov.uk
- DfE Generative AI: product safety expectations: www.gov.uk