Holly Hill Primary and Nursery School

Online Safety Policy

October 2026

Order of contents

- **General statement**
- **Legal framework and guidance**
- **Purpose of this policy**
- **Roles and responsibilities**
  - Governing body
  - Head Teacher
  - Designated Safeguarding Leads
  - Computing Leaders
  - All staff members
  - Pupils
- **Teaching Methods**
- **Online Safety Training for Staff**
- **Online Safety and the Curriculum**
  - Education of pupils
  - Education of parents/carers
- **Record keeping and assessment**
- **Acceptable use of technologies**
  - Photographic, video and audio technology
  - Internet/website content incl. school website
  - Email management
  - Use of mobile phones
  - Social media/Social networks
  - Chat and instant messaging
  - Generative artificial intelligence (Gen AI)
- **Handling online safety concerns, complaints (incl. illegal incidents)**
  - Cyberbullying
  - Child-on-child abuse (including violence and harassment)
  - Child sexual exploitation (CSE)
  - Child criminal exploitation (CCE)
  - Cyber-crime (cycle-enabled/cyber-dependent)
  - Grooming and exploitation
  - Mental Health
  - Online hoaxes and harmful online challenges
  - Radicalisation
  - Network security
  - Cyber Security
  - Filtering and monitoring online activity
- **Reporting misuse**
- **Remote Learning**
- **Data Protection**

General Statement

The use of digital technologies/online services is a crucial aspect of everyday life. To ensure that the children are well-supported and have a clear understanding of using digital technologies appropriately and safely, staff work closely with the children and parents to ensure that children are using online services in a safe way and know how to deal with situations such as online bullying. External guidance has been considered, to help write this policy. This policy applies to all members of Holly Hill Primary School community (including staff, pupils, parents/carers, volunteers/workplace students, visitors and community users) who have access to and are users of school digital systems, both in and out of School and the use of personal digital technology on the school site (where allowed).

Legal Framework and Guidance

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

- The UK General Data Protection Regulation (UK GDPR)
- The Data (use and access) Act 2025 (DUAA)
- Data Protection Act 2018
- Computer Misuse Act 1990 / Serious Crime Act 2015
- Communications Act 2003
- Counter Terrorism and Securities Act 2015
- Education and Inspection Act 2026
- Revised Prevent Duty for England and Wales 2023
- Voyeurism (offences) Act 2019
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2026) 'Keeping children safe in education'
- DfE (2023) 'Teaching online safety in school'
- DfE (2026) RSE and Health Education
- DfE (2018 updated 2026) Working together to safeguard children
- DfE (2026) 'Filtering and monitoring standards for schools and colleges'
- DfE (2024) 'Cyber Security Standards for schools and colleges'
- DfE (2025) 'Generative artificial intelligence (AI) in education'
- DfE (2026) Generative AI ;-product safety standards
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2026) 'Meeting digital and technology standards in schools and colleges'
- DfE (2026) Mobile phones in schools guidance
- UK Council for Internet Safety (2020) Education for a connected world
- National Cyber Security Centre
- Online Safety Act 2023

This policy operates in conjunction with the following school policies:

- Social networking sites within Staff code of Conduct & Parent / Carer Code of Conduct Policy
- Anti-Bullying Policy
- Acceptable Use Agreements (Pupils, Staff, Governors, Volunteers, Parents / Carers)
- Behaviour Policy
- Child Protection Policy
- Child-on-child Abuse Policy
- GDPR policies (inc Acceptable Personal Use of resources and Assets Policy (C5), Data Handling Security Policy (C6) and privacy notices (Section D)
- Personal Social Health Education Policy (inc RSE)

- Prevent Duty Policy
- Allegations of Abuse Against Staff Policy
- Remote Learning Policy
- Cyber Security Policy and Cyber Response and Recovery Plan
- Filtering and Monitoring Policy
- Mobile Phone Policy (Primary School)

The purpose of this policy is to:

- To set out the key principles expected of all members of the school community at Holly Hill Primary School with respect to the use of online services and digital technologies.
- To safeguard and protect the children and staff of Holly Hill Primary School.
- To assist school staff working with children to work safely and responsibly with online services and other communication technologies.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the online services and digital technologies for educational, personal or recreational use.
- To have clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To ensure a whole school approach to online safety.
- To set out reporting, recording and response procedures for online safety incidents.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices including the use of AI by all pupils and staff. The Online Safety Policy is part of the schools safeguarding framework and should be read alongside Child Protection Policy, Behaviour Policy, Anti-bullying Policy, Acceptable use Policy and Data Protection Policies.
The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: **How to evaluate what they see online. To enable pupils to make judgements about what they see** e.g. being exposed to illegal, inappropriate or harmful material or content, e.g. AI - generated content, pornography, misinformation, disinformation (including fake news), conspiracy theories, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: **How to identify possible online risks and make informed decisions about how to act. How to assess a situation and think through the consequences** e.g. being subjected to harmful online interaction with other users or generative AI applications, e.g. peer to peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: **To enable pupils to understand what acceptable and unacceptable online behaviour looks like and that the same standard is expected online as offline** e.g. personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit images / videos including those generated using AI, messages and cyberbullying.
- **Commerce: How to recognise techniques used for persuasion. To enable pupils to recognise the techniques that are often used to persuade or manipulate others** e.g. risks such as online gambling, inappropriate advertising, phishing and /or financial scams.

Other areas include managing online information, copyright and ownership and privacy and security.

Roles and responsibilities

The governing body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- The approval of the online safety policy on an annual basis.
- Monitoring, reviewing and evaluating online safety provisions, issues or incidents including filtering and monitoring systems and to challenge its effectiveness.
- Ensuring all staff undergo safeguarding and child protection training, including online safety.
- Ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils and staff.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed and recorded at least annually in liaison with DSL- Mrs Leal, SLT – Mrs Steed, Computing lead staff and ICT service providers.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Taking part in online safety training/awareness sessions.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.
- The nominated Governor is Robin Edwards.

The Head Teacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Ensuring staff receive regular, up-to-date and appropriate online safety training including filtering and monitoring information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited, evaluated and procedures are in place for reporting incidents and inappropriate internet use, either by pupils or staff. That government guidance and previous incident reviews support the improvements of procedures.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety, including it being tailored to the specific needs and vulnerabilities of individual children.
- Ensuring online safety concerns / incidents are recorded using CPOMS and entries monitored and actions taken as required.
- Working with other DSLs and ICT staff / Technical support and the governing body to review policies and procedures including reports generated that supports online safety.
- Ensuring parents / carers have opportunities to be engaged with online safety information and events.

The designated safeguarding leaders are responsible for:

- Taking the lead responsibilities for safeguarding and child protection which includes undertaking training to support a good knowledge of their own role. Also, they are able to understand the unique risks associated with online safety to keep children safe whilst they are online at school. This will also include recognising additional risks that vulnerable pupils face online.
- Working with other agencies with regard to online safety incidents.
- Ensuring online safety is recognised as part of the school's ongoing safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring incidents are recorded and reviewed (including actions) using CPOMS.
- Understanding the filtering and monitoring systems and processes in place at school and ensuring they continue to meet the schools' safeguarding needs.
- The nominated DSL is Mrs J Leal.

Computing Leaders are responsible for:

- Working with the DSL Team to review and update information obtained from CPOMS with regard to online safety incidents as required.
- Working with the DSL Team/PSHE leader to develop a planned and coordinated online safety education for pupils e.g. Project Evolve, Tech She Can, Google Legends, Jigsaw PHSE scheme and the use of AI.
- Liaising with relevant members of staff / agencies to respond to online safety incidents, gaps in school provision and use this to update the school's procedures.

All staff members are responsible for:

- Being alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents in line with school policies.
- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Reading, understanding and signing the staff acceptable use agreement and following other relevant policies eg Online Safety policy and Child Protection policy.
- Modelling good online behaviours and challenging harmful online behaviour and to report concerns.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an up-to-date awareness of online safety, emerging online safety issues and of the current school online safety policy and practices.
- Undertaking Prevent duty and safeguarding training as needed.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure including recording incidents via CPOMS using the online safety / issues tab.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Prior to using websites, tools, apps, AI systems or other online platforms in the classroom, or recommending that pupils use these platforms at home, staff will review and evaluate the resource.
- Ensuring that any internet-derived materials/ AI tools are used in line with copyright law.
- Supervising pupils when using technologies during lesson time – this supervision is suitable to their age and ability and follows procedures for online safety issues.
- Understanding that filtering and monitoring supports – but does not replace- effective supervision, professional curiosity and safeguarding judgement.
- Using school approved digital services and AI tools to protect data and verify AI outputs for accuracy / bias before use.

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.
- Understanding that out-of-school behaviour may be addressed where it affects the school community.

Teaching Methods

We use the National Curriculum incl. RSE Health Education statutory guidance 2026, Education for a Connected World 2020 edition, Project Evolve, NCCE Teach Computing, Google Legends and Jigsaw PSHE to allow the children to progress their skills throughout their time at Holly Hill Primary School. These will be implemented into our planning to plan engaging lessons which may include the use of technology or creative computational thinking through practical activities. Online safety skills are included within both the computing and PSHE curriculum and cross curriculum areas as appropriate and should be regularly revisited

Online Safety Training for Staff

The Head Teacher / DSL Team will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Online Safety and the Curriculum

This is based on the 4C's – see page 4 – purpose of this policy.
Through our curriculum, we will teach the children the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently, regardless of the device, platform or app. This includes how to use technology safely, responsibly, respectfully and securely, and know where to go for help and support. Pupils are also 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.

Children should (based on the SMART rules):

- *Know that personal information should be kept private. (Safe)*
- *Know not to meet anyone they have met online, that they do not know in person without parents' permission. (Meet up)*
- *Know not to accept any files, images or downloads from a stranger as they may contain viruses. (accepting)*
- *Be able to recognise and identify that everything on the internet is not always true. (Reliable)*
- *Always tell a responsible adult if anything makes them feel uncomfortable or worried. (Tell)*

All areas will be taught alongside our Jigsaw PSHE scheme including Relationship Education (topics in brackets below) and within our computing curriculum:

Self-Image and Identify (Celebrating Difference, Relationships)

Online Relationships (Relationships, Healthy Me, Changing Me, Celebrating Difference, Being me in my world)

Online Reputation (Relationships, Healthy Me)

Online Bullying (Celebrating Differences, Healthy Me, Relationships, Changing Me)

Health, Well-being and Lifestyle (Healthy Me, Celebrating Difference, Relationships, Changing Me)

Privacy and Security (Relationships)

Managing Online Information (Celebrating Difference, Healthy Me, Relationships, Changing Me)

Copyright and Ownership (Relationships)

Education of pupils

Online safety teaching is always appropriate to pupils' ages and developmental stages.
Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.
Pupils will be taught to take a responsible approach, think critically, develop informed decisions and build their resilience to online safety risks.

Pupils are aware of their responsibilities regarding the use of school-based systems and equipment including their expected behaviour outlined in the acceptable use agreement (class or individual).

The school recognises that, while any pupil can be vulnerable online and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstances and there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. The SENCO/SEND Team or Computing leads can support with differentiation, so pupils receive the information and support they need. The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

The following resources can help to support vulnerable pupils stay safe online:
- Vulnerable Children in a Digital World - Internet Matters (PDF)
- Google Legends – Legendary SEND pack
- Children's online activities, risks and safety - A literature review by the UKCCIS Evidence Group section 11 (2017)
- STAR SEND Toolkit – Childnet (11-16yrs old)
- NSPCC – online safety for families and children with SEND

Education of parents / 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 works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents are sent a copy of both the pupils and parents acceptable use agreement during the first term of the school year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.
Parents are aware of ways to support online safety via the acceptable use agreements, school web site information including policies and school-based information, information posters, newsletters or events e.g. national online safety campaigns, digital parenting magazines or Parent Zone.

Record Keeping and Assessment

When online safety is included in specific computing blocks (NCCE/Teach Computing) staff will use their assessment judgements to complete an evaluation of the learning in that computing unit, which is submitted to the subject leader. Where gaps or issues have been identified these will be acted upon through adaptation of later units, adaptation of planning, further knowledge reviews.
Staff review and reflect upon pupil's knowledge and learning through observations, discussions, quizzes, knowledge maps on Project Evolve and the implementation of the feedback policy.

Acceptable Use of Technologies (also see school acceptable use policies)

Photographic, video and audio technology

- Staff and pupils must take care when capturing photographs or videos to ensure that all pupils are appropriately dressed.
- Staff will use school photographic or video devices to support school trips and curriculum activities.
- Pupils should always seek the permission of their teacher before taking photographs, making audio or video recordings within school.
- Inappropriate material must be reported to a responsible adult and should not be downloaded onto school hardware.
- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images or that of others, on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press.

Internet/Website Content incl. the School website

- If staff or pupils discover unsuitable websites, the web address (URL) and content must be reported to the Head Teacher (Mrs Leanne Steed).
- Staff and pupils must ensure that their use of internet derived materials complies with copyright law. Pupils will be taught to acknowledge the source of information used and to respect copyright.
- The point of contact on the website will be the school address, school e-mail and telephone number. Staff personal information will not be published.
- Images and videos are only posted on the website if the correct media type permissions have been given.

Also see section - photographic, video and audio technology

- Website photographs will be carefully selected and will only show pupils whose parents have given permission for their photographs to be used. Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- When publishing materials to websites and elsewhere, staff and pupils should consider the thoughts and feelings of those who might view the material.
- Material that victimises or bullies someone else, or is otherwise offensive, is unacceptable.
- The Head Teacher will take overall editorial responsibility for the website and ensure that content is accurate and appropriate and meets government requirements.
- (Also see section on managing filters)

Email management

- Access to and the use of emails will be managed in line with Data Protection and Acceptable Use Policies.
- Personal e-mail or messaging between staff and pupils should not take place.
- Staff are given approved school email accounts with password protection / multi factor authentication.
- Staff members will be required to block spam and junk emails and be aware of how to recognise potential phishing / malicious emails and how to report such emails. (in person / via device)
- Information and awareness regarding phishing / malicious emails etc will be shared with the pupils through online safety and the curriculum.

Use of mobile phones

- Any pupils' phones brought into school will be kept in the school office during the school day.
- Pupils must not use or access mobile phones or similar smart devices at any point during the school day, regardless of location on the school site. Pupils are discouraged from bringing mobile phones to school. If a pupil breaches the policy, the phone will be confiscated and returned to a parent / carer where appropriate at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.
- Mobile phone cameras should not be used inappropriately and photographs should not be forwarded to unknown sources.
- Also see the specific Mobile Phone policy (Primary School) 2026.

Social Media/Social Networks

- Use of social media on behalf of the school will be conducted by the Head Teacher or designated members of staff.
- Access to social networking sites is filtered as appropriate.
- Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school – also see Acceptable Use Policy.
- Concerns regarding the online conduct of any member of the school community on social media are reported to the Head Teacher.

Chat and instant messaging

- Pupils will not be allowed access to public or unregulated chat rooms.
- Pupils will not access social networking sites within school.

- Any form of bullying or harassment is strictly forbidden and must be reported immediately if this does arise.
- A risk assessment will be carried out before pupils are allowed to use a new technology in school.

Generative artificial intelligence (Gen AI)

- The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.
- The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation to support this.
- We will recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding / child protection, data protection and technical security arrangements, and by updating procedures. Filtering and monitoring procedures, reviews and checks help limit the pupil's ability to access or create harmful or inappropriate content through generative AI.
- KCSIE 2026 recognises that learners and staff may be subject to harmful online interactions with other users or generative AI applications that simulate these.

Handling online safety incidents, concerns, complaints (incl. illegal incidents)

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils.
- The school will take all reasonable precautions to ensure online safety. However, due to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Methods to identify, assess and minimise risks will be reviewed regularly. The filtering and monitoring of online activity support the restrictions to any websites that involve gambling, games, financial scams, pornography and adult material.
- Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Following an incident, staff will: -

- Inform the Head Teacher / DSL Team. They will investigate the concern or online behaviour inline with school policies and share with relevant staff as required.
- Log a record of the incident using the CPOMs system under Online Safety concern tab
- Inform parents or carers as needed

Our Head Teacher acts as first point of contact for any complaint. Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school/LEA child protection procedures.

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Concerns regarding a pupil's online behaviour are reported to the DSL Team via the school system CPOMS. This will be followed through via relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern or suspicion that the web site(s) concerned may contain child abuse images or if there is any other suspected illegal activity or materials related to or responding to online safety incidents having taken place, the Head Teacher or DSL Team will report this immediately to the police in line with safeguarding arrangements.
If during the review of incidents any illegal materials are found or suspected, the school investigation will be halted and evidence secured and preserved e.g. isolate the computer and await the police response.

Concerns regarding a staff member's online behaviour are reported to the Head Teacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, Acceptable Use Agreement Policy and Disciplinary Policy and Procedures. If the concern is about the Head Teacher, it is reported to the Chair of Governors.

Cyberbullying
Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy. The school are aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Child-on-child abuse (including harassment and violence)
Pupils may also use the internet and technology, including AI generated or altered images as a vehicle for harmful sexual behaviours. Staff will be aware of the indicators of abuse, neglect and exploitation. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The school responds to all concerns regarding online child-on-child abuse (including harassment and violence), regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL Team, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)
Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.
CCE is also a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. It is increasingly common for children to be groomed and manipulated into participating through the internet.
Any concerns will be report by staff to the DSL Team in line with policies.

Cyber-crime
Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL Team will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests. Staff and pupils will understand the basics of cyber security and ways to protect themselves from cybercrime in line with the Cyber Security Policy.

Grooming and exploitation
Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.
Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons.
This awareness is raised through training events and information in line with our child protection policy.

Mental health
The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.
Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively.

This awareness is raised through training events and information in line with our child protection policy / PSHE policy.

Online hoaxes and harmful online challenges
For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.
For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.
Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL Team immediately.

Radicalisation
Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological. Concerns will be handled in line with Prevent Duty Policy.

Network security
Technical security features, such as anti-virus software, are kept up-to-date and managed by ATOM IT. Firewalls are switched on at all times and updated / managed by ATOM IT to ensure they are running correctly.
All members of staff have their own unique usernames and private passwords to access the school's systems as required. These also have enforced password protection policies and multifactor authentication (MFA) as required. Users will be required to lock access to devices and systems when they are not in use. Arrangements are in place to provide supply staff with appropriate access to systems which expire after set use. Access rights to both physical and cloud-based school technical systems and devices are based on roles and responsibilities.
Additional details of the school's network security measures can be found in GDPR Policies C5, C6 or from the DPO.

Cyber security
School recognises cyber threats including phishing, ransomware, malware and unauthorised access to data.
Senior leaders and governors understand cyber risks and their safeguarding implications receive appropriate assurance.
Staff receive regular cyber-security training covering phishing, credential theft, malicious links, social engineering, ransomware, AI-enabled scams and other emerging threats.
Pupils receive age-appropriate education about cyber security, scams, account protection and the lawful and responsible use of systems.
Cyber security arrangements are kept under regular review and updated in line with emerging risks or sooner if required by incidents.

Filtering and monitoring online activity
The school's governing body will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges. The governing body will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
Filtering and monitoring systems are managed to ensure they meet the school's safeguarding needs, with a co-ordinated approach by assigned staff, governors and our IT support providers Atom IT.
The school's technical infrastructure and systems have appropriate levels of filtering managed by Atom IT to ensure that children and users are safe from terrorist and extremist material when accessing the internet

within school. Physical monitoring by staff when pupils are using devices supports the technical monitoring services.
Named staff are responsible for making sure checks are made to ensure filtering methods selected are appropriate, effective and reasonable. (This may include running key word searches on Google or other search engines images prior to the lesson to check content is appropriate.)
Reports from staff or parents of inappropriate websites or materials will be made to the Head Teacher / DSL Team or Computing Leaders immediately, who will investigate the matter and makes any necessary changes in consultation with IT support providers. (Atom IT)
The school will work in partnership with the LEA, Governors, Staff and our ICT technical support, currently Atom IT, to ensure systems to protect pupils are effective, appropriate and reviewed regularly – at least annually.
If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.
The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the Head Teacher / DSL Team who will manage the situation in line with the Child Protection and Safeguarding Policy.
Reviews and checks of the effectiveness of the filtering and monitoring systems will be carried out on different device types and users. This will be reviewed and logged at least once every academic year to demonstrate procedures.

Reporting misuse

Inappropriate activities are discussed and the reasoning behind these prohibiting activities due to online safety are explained to pupils as part of the curriculum in order to promote responsible internet use.
Any instances of misuse by pupils should be reported to the class teacher who will then report to the Head Teacher.
If a pupil does not adhere to the acceptable use agreement parents/carers will be informed following discussion with the Head Teacher.
Complaints of a child protection issue shall be dealt with in accordance with the school child protection policy.
Any instances of misuse by staff, visitors, or governors should be reported to the Head Teacher/ Chair of Governors as required in line with the acceptable use agreement and other relevant policies.

Remote Learning

All remote learning will be delivered in line with the school's Remote Learning Policy which includes the use of school devices.

Data Protection

The school has:

- a range of Data Protection Policies and Privacy Notices. (some available on the school website)
- implemented the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- paid the appropriate fee to the Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- acknowledged that changes in technology, emerging safeguarding risks, national guidance and statutory expectations will be reflected within this policy.

Date of policy updated:	October 2026
To be reviewed:	October 2027
Governing Body meeting	October 13th 2026

This policy may be reviewed before this date with regard to when any significant changes occur with technologies used within school.