PENNTHORPE
NURSERY PRE-PREP PREP

ONLINE SAFETY POLICY 2025 – 2026

THIS POLICY INCLUDES EARLY YEARS FOUNDATION STAGE

Policy Author:	Head of School – Jon Marler
Date reviewed by author:	August 2025
Next review date:	September 2026

Governor sign – off		
Governor: Iain Regan-Smith	Date:	04/11/2025

1. Introduction

The school does not permit pupils to bring into school or use mobile phones in school.
This Online Safety Policy should be read in conjunction with the school's Safeguarding and Child Protection Policy and the Staff and Pupil Acceptable Use Agreements.

The school ensures that online safety is a running and interrelated theme across the school and is considered in all school policies and procedures, including planning the curriculum, teacher training, the role of the DSL's and parental engagement.

Online Safety encompasses not only the internet but also wireless electronic communications including mobile devices, games consoles, cameras and web-cams. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using IT. In many areas technology is transforming the way that schools teach and how children learn. At home, technology is changing the way children live and with the activities they choose, these trends are set to continue.

Therefore, the purpose of the policy is to:

- Prevent online harm and abuse
- Promote safe, appropriate and productive use of online resources
- Set out the key principles expected of all members of Pennthorpe School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff from potentially harmful and inappropriate online material, in-line with the school's Safeguarding and Child Protection Policy and the Keeping Children Safe in Education 2025 (KCSIE) guidelines.
- Have clearly defined roles and responsibilities for online safety.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Set out clear expectations for any visitors or guests accessing the school network and IT equipment.
- Details on how the school builds resilience in its pupils and how the school informs and educates parents in online safety.

- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies (Anti-Bullying and Cyber-Bullying Policy).
- 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.
- Minimise the risk of misplaced or malicious allegations made against adults who work with children.
- Details of the school monitors and filters inappropriate content.

2. Key risks

The breadth of risks related to online safety is considerable but is categorised into four key areas as follows:

Content:
Being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact:
Being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

Conduct:
Personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

Commerce:
Risks such as online gambling, inappropriate advertising, phishing and or financial scams. If we feel our pupils, or staff are at risk, a report will be made to the Anti-Phishing Working Group (https://apwg.org/).

3. Reviewing and monitoring online safety:

The school conducts an annual review of its approach to online safety.

4. Key roles and responsibilities:

Everyone in the school community has a responsibility to ensure that they are aware of the potential benefits and risks associated with modern technology. Staff should follow the school's procedure concerning electronic devices and know how to deal with Online Safety incidents according to the Online Safety policy. There are, however, key roles for members of staff to produce and monitor the school Online Safety policy. They are as follows:

The Welfare Committee:

- Comprising of the Designated Safeguarding Lead (DSL), Deputy DSL's as well as the Head of Digital learning; the committee will oversee all aspects of Online Safety within the school and report, via the Head of School, on an annual basis, to the school's Governing Body.

The Head of School:

- To take overall responsibility for Online Safety provision.
- To take overall responsibility for data and data security.
- To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements.
- To be responsible for ensuring that staff receive suitable training to carry out their Online Safety roles and to train other colleagues, as relevant.
- To be aware of procedures to be followed in the event of a serious Online Safety incident.

The Head of Digital Learning:

- Takes on day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies/documents.
- Promotes an awareness and commitment to E-Safeguarding throughout the school community.
- Ensures that Online Safety education is embedded across the curriculum.
- To communicate regularly with the Designated Safeguarding Lead to discuss current issues, review incident logs and filtering / change control logs.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident.
- To ensure that an Online Safety incident log is kept up to date.
- Facilitates training and advice for all staff.
- Is regularly updated in E-Safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming
    - cyber-bullying and use of social media
    - extremist and terrorist behaviour

5. Additional roles and responsibilities:

Teaching and Support Staff:

- Have an up-to-date awareness of Online Safety matters through appropriate and effective training and of the current school's Online Safety policy and practices.
- Have read, understood and signed the school's Acceptable Use Policy.
- Report any suspected misuse or problem to the DSL or Head of School.
- Ensure that communications with pupils (email etc.) should be on a professional level and carried out using only official school systems.
- Ensure that Online Safety issues are embedded into the curriculum and other school activities.

- Embed Online Safety issues in all aspects of the curriculum and other school activities.
- Supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).

Network Manager & IMS (External IT Support Contractors)

- Report any Online Safety related issues that arise, to the DSL and Online Safety DSL.
- Ensure that users may only access the school's networks through an authorised and properly enforced password protection policy.
- Ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date).
- Ensure the security of the school's IT system.
- Ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices.
- Apply and update the school's policy on web filtering on a regular basis.
- That he/she keeps up to date with the school's Online Safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- Keep up-to-date documentation of the school's e-security and technical procedures.

All Staff:

- To read, understand and help promote the school's Online Safety policies and guidance.
- To read, understand, sign and adhere to the school's Acceptable Use Policy.
- To be aware of online safety issues related to the use of personal mobile devices and that they monitor their use and implement current school policies with regard to these mobile devices.
- To report any suspected misuse or problem to the DSL and/or Head of School.
- To maintain an awareness through appropriate and effective training of current online safety issues and guidance.
- To model safe, responsible and professional behaviours in their own use of technology.
- To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g., email, text, mobile devices etc.

Pupils:

- To read, understand, sign and adhere to the Acceptable Use Policy (within Pre-Prep it would be expected that parents/carers would read these with their children and sign on behalf of the pupils).
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials.
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology.

- Should not bring personal mobile devices into school, unless previously agreed with the Network Manager.
- To know and understand school policy on the taking/use of images and on cyber-bullying.
- To 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.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home to help the school in the creation/review of E-Safety policies.

Parents/Carers:

- To support the school in promoting e-safety and endorse the Acceptable Use Policy which includes the pupils' use of the internet and the school's use of photographic and video images.
- To access the school website /learning platform/on-line student/pupil records in accordance with the relevant school Acceptable Use Policy.

To consult with the school if they have any concerns about their children's use of technology.

6. Teaching and learning of online safety:

Why internet and digital communications are important:

- The internet is an essential element in 21st century life for education, business and social interaction.
- The school has a duty to provide pupils with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Pupils will be taught what internet use is acceptable, and what is not, and given clear objectives for internet use.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be shown how to publish and present information appropriately to a wider audience.
- Pupils will occasionally take part in Online Safety workshops run by outside agencies.
- Pupils will occasionally take part in Safer Internet Day each year.
- Pupils will be taught how to evaluate internet content.
- The school will seek to ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant internet content e.g., using the CEOP.
- For children with social, familial or psychological vulnerabilities, further consideration should be taken to reduce potential harm.

7. Managing internet access:

Information security:

- School IT systems security will be reviewed regularly.
- Virus protection will be updated regularly.

E-mail:

- Staff may only use approved e-mail accounts on the school system.
- Pupils have school email accounts and should only communicate with staff via these accounts.
- Staff to pupil email communication is only permitted as per the Staff Code of Conduct, using school email accounts.
- Incoming e-mail should be treated as suspicious, and attachments not opened unless the author is known.

Published content and the school web site:

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.

The Head of School or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work:

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children.
- Pupils' full names will be avoided on the website or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Parents should be clearly informed of the school's policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing on the school learning platform:

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords. This control may not mean blocking every site it may mean monitoring and educating pupils in their use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of opportunities; however, it does present dangers for primary and secondary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Staff should follow the social networking guidelines as set out in the Staff Code of Conduct and Acceptable Use Policy.

Extremist material:

- Extremist material and access to it is an increasing national threat and the school takes its responsibility in protecting the school and the children seriously. The school filters, screen captures and email filters help protect the children by blocking inappropriate content and flagging worrying behaviour in this area to the child protection lead.
- Teaching staff undergo relevant training, for example Channel to raise their awareness of the risks posed by online activity of extremist and terrorist groups and to help support and protect the children in their care.

8. Managing Access:

Monitoring

- Monitoring involves tracking and reviewing user activity to identify potential safeguarding concerns. This includes flagging keywords, unusual behaviour, or attempts to bypass filters.
    - Example: Alerting staff if a student searches for self-harm content or uses concerning language in messages.
- Pennthorpe manage their own school monitoring and filtering through Smoothwall.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Network Manager.

Filtering

- Filtering refers to the blocking or restricting access to harmful or inappropriate online content. This includes websites, images, and search results that may pose a risk to students.
    - Example: Preventing access to gambling sites or extremist content.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Devices are only filtered whilst connected to a school managed internet connection. When offsite, it is the responsibility of the children and parents to safeguard and monitor age-appropriate content.

9. Managing emerging technologies:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- In rare cases where a pupil has been granted permission to have a device at school any mobile devices and associated cameras will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Handheld technologies, including games and mobile devices, often have internet access which may not include filtering.
- Staff will use a school phone where contact with pupils is required.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

10. Authorising internet access:

- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- In Pre-Prep and Lower Prep, access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Assessing Risks:

- The school will carry out regular audits of risks and take any appropriate actions.
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will monitor IT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

Handling E-Safety Complaints:

- Complaints of internet misuse must be referred to the Network Manager, Head of Digital Learning, DSL and/or the Head of School.
- Any complaint about staff misuse must be referred to the Head of School.
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the school's Behaviour Management and Sanctions Policy.

Community Use of the Internet:

All use of the school internet connection by community and other organisations shall be in accordance with the school Online Safety Policy.

11. Expectations of staff, pupils and parents

Introducing the Online Safety & Acceptable Use policies to pupils:

- Appropriate elements of the Online Safety & Acceptable Use policies will be shared with pupils.
- For remote learning, the school has a separate 'Pupil Code of Conduct for remote Learning' which is issued and discussed with all pupils on commencement of a remote learning period or academic year (whichever applies).
- Pupils will be informed that network and internet use will be monitored.
- Curriculum opportunities to gain awareness of Online Safety issues and how best to deal with them will be provided for pupils in all year groups, regularly throughout the school year. This should be addressed each year as pupils become more mature and the nature of newer risks can be identified.
- Children will occasionally attend Online Safety workshops run by outside agencies.
- Each year all children will take part in Safer Internet Day.

Staff and the Online Safety & Acceptable Use Policy:

- All staff will be given the School Online Safety Policy & Acceptable Use Policy and their importance explained.
- All staff will sign to acknowledge that they have read and understood the Online Safety & Acceptable Use Policies and agree to work within their agreed guidelines.
- All staff should complete an asset log of any IT equipment they have on loan.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential in line with the Staff Code of Conduct.
- Staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff will regularly receive E Safety and Safeguarding Training.

Enlisting Parents' Support:

- Parents' and carers' attention will be drawn to the Online Safety & Acceptable Use policies in newsletters and on the school web site.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.
- Parents should be given Online Safety training with a focus on education and having an overview of the tools to allow them to take control whilst not undermining trust. Parent Online Safety presentations, workshops and coffee clinics will take place occasionally. These will be delivered by outside agencies as well as the Head of Digital Learning and the Head of School.
- The school would encourage Parents to talk to their children about their online activity and potential rules for their household.
- Often children do not wish to be constantly online but often lack sufficient alternatives for play, travel interaction and exploration. Parents should be encouraged, where possible to interact with their children on the internet as well as provide other opportunities for learning and recreation.

12. Illegal and inappropriate activities by staff or pupils

- Pennthorpe believes that the activities listed below are inappropriate in a school context and that users should not engage in these activities when using school equipment or systems (in or out of school).
- Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:
    - Child sexual abuse images (illegal -The Protection of Children Act 1978).
    - Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003).
    - Possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008).
    - Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986).
    - Pornography or inappropriate sexual images.
    - Promotion of any kind of discrimination.
    - Promotion of racial or religious hatred.

- Promotion of extremism or terrorism.
- Threatening behaviour, including promotion of physical violence or mental harm.
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

Additionally, the following activities are also considered unacceptable on IT equipment provided by the school:

- Using school systems to run a private business.
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords).
- Creating or propagating computer viruses or other harmful files.
- Carrying out sustained or instantaneous high-volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet.
- Online gambling and non-educational gaming.
- Use of personal social networking sites/profiles for non-educational purposes.

IT users must:

- Not search for or use websites that bypass the school's internet filtering.
- Not download or even try to download any software without the explicit permission of a member of the IT systems support department.
- Not attempt to install unauthorised and unlicensed software.
- Be extremely cautious about revealing any personal details and never reveal a home address or mobile telephone number to strangers.
- Not use other people's user ID or password, even with their permission.
- Not interfere with or cause malicious damage to the IT Facilities.
- Report any breach (deliberate or accidental) of this policy immediately.

13. Reporting inappropriate use and sanctions:

It is more likely that Pennthorpe will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

For staff and pupils, Pennthorpe School reserves the right to access all material stored on its IT system, including that held in personal areas of staff and pupil accounts for purposes of ensuring school policies regarding appropriate use, data protection, computer misuse, child protection, and health and safety are adhered to.

Pupils who are found not to be acting responsibly in this way will be sanctioned using the school's Rewards and Sanctions Policy. Irresponsible users will be denied access to the IT facilities. The Safeguarding and Child Protection Policy will be adhered to where a child is considered to be at risk or placing others at risk.

Staff who are found not to be acting responsibly to breaching expectation may be disciplined as outlined in the Staff Handbook.

Pennthorpe School will act strongly against anyone whose use of IT risks bringing the school into disrepute or risk the proper work of other users including taking legal action.

14. Equipment and digital content:

Staff Use of Personal Mobile Devices:

- Staff's personal handheld mobile devices, including mobile phones, personal iPads or cameras **must be not be** used for photographing children.
- Staff in Early Years Foundation Stage are required to store personal mobile phones and other mobile devices in a storage cupboard away from the direct working area with the children.
- Staff are not permitted to use their own mobile phones or mobile devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Mobile phones and personally-owned mobile devices may not be used during lessons or formal school time.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

Pupils' Use of Personal Mobile Devices:

Pupils are not permitted mobile phones at Pennthorpe.

- No personal mobile devices, including phones, and iPads are permitted in school. Extreme cases will be considered and this must be previously agreed by the Head of Digital L and/or the Head of Year and/or Head of School.
- If a pupil breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and mobile devices will be released to parents or carers in accordance with the school policy.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile device during the school day if they have permission to bring this to school, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned mobile devices, and will be made aware of boundaries and consequences.

15. Digital images and video:

At Pennthorpe:

- We gain parental carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil permission for its long-term use.
- The school blocks/filters access to social networking sites and/or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught how images can be manipulated in their Online Safety education lessons and also taught to consider how to publish for a wide range of audiences which might include Governors, parents or younger children as part of their IT scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

16. Generative Artificial Intelligence

Generative AI tools, such as chatbots, image generators, and automated content creation platforms, are increasingly present in educational contexts. While these technologies offer opportunities for enhanced learning and creativity, they also pose risks related to misinformation, data privacy, and exposure to inappropriate content.

Pennthorpe recognises the importance of managing the use of generative AI responsibly and in line with statutory guidance, including the Department for Education's expectations and the Online Safety Act.

Use and Oversight:

- Any use of generative AI tools within the school must be approved by the Head of Digital Learning in consultation with the DSL and IT support team.
- The School has a licensed version of CoPilot – All other generative AI will be blocked by the School filtering system.
- Staff must not use generative AI tools with pupils unless the tool has been assessed for safety, educational value, and compliance with data protection standards.
- Pupils must be supervised when engaging with AI tools and taught to critically evaluate AI-generated content.

Risk Assessment and Compliance:
All AI tools used in school will be assessed against the DfE's guidance on generative AI, including:

- Content filtering and moderation capabilities.
- Logging and monitoring of interactions.
- Data security and privacy safeguards.
- AI tools must not be used to generate or disseminate misleading, biased, or harmful content.

Training and Education:

- Staff will receive regular training on the safe and ethical use of generative AI, including recognising risks and safeguarding concerns.
- Pupils will be educated on the limitations of AI, the importance of verifying information, and the ethical considerations of using AI-generated content.
- Parents will be informed about the school's approach to AI and provided with resources to support safe use at home.

Monitoring and Review:

- The use of generative AI will be reviewed annually as part of the school's Online Safety Audit and risk assessment.
- Any incidents involving misuse of AI tools will be logged and addressed in accordance with the school's safeguarding and disciplinary procedures.

17. Misinformation, Disinformation, and Conspiracy Content

In line with the latest guidance from Keeping Children Safe in Education (KCSIE) 2025 and the Online Safety Act, Pennthorpe recognises the growing risks posed by misinformation, disinformation, and conspiracy content online. These forms of digital harm can undermine pupils' understanding of the world, distort facts, and contribute to unsafe or radicalised behaviours.

Definitions:
Misinformation refers to false or misleading information shared without harmful intent.

Disinformation is deliberately false information spread with the intention to deceive or manipulate.

Conspiracy content includes unfounded or harmful theories that may promote distrust, extremism, or anti-social behaviour.

Curriculum Integration:

- Pupils will be taught to critically assess online sources, verify facts, and recognise bias or manipulation.
- Online safety education will include examples of misinformation and conspiracy theories, with age-appropriate discussions on their impact.
- Staff will be supported to embed these themes across subjects, including PSHE, humanities, and digital learning.

Staff Training:

- Staff will receive regular updates on emerging online harms, including misinformation and disinformation. This will be done through Staff Briefings, EduCare, e-mail notifications and any other appropriate mediums

Monitoring and Response:

- Any incidents involving pupils sharing or engaging with harmful misinformation or conspiracy content will be logged and addressed in line with safeguarding procedures.
- The school will work with parents to raise awareness and provide guidance on managing exposure to misleading content at home.

Parental Engagement:

- Parents will be offered resources and workshops to help them understand the risks of misinformation and conspiracy content.
- The school will encourage open dialogue between pupils and parents about online content and digital safety.

18. Cybersecurity Standards

Pennthorpe recognises that robust cybersecurity is essential to safeguarding pupils, staff, and school data. In line with the expectations set out in Keeping Children Safe in Education (KCSIE) 2025 and the Online Safety Act, the school is committed to implementing and maintaining cybersecurity measures that align with the standards recommended by the National Cyber Security Centre (NCSC).

Cybersecurity Measures:

The school adopts NCSC-aligned standards, including:

- Strong access controls and password policies.
- Regular software updates and patching.
- Antivirus and anti-malware protection across all devices.
- Encryption of sensitive data stored or transmitted electronically.
- All staff and pupils must follow the school's Acceptable Use Policy and report any suspected breaches or vulnerabilities immediately.

Monitoring and Audits:

- The IT support team maintains logs of system access, filtering changes, and incident reports.
- Cybersecurity risks are reviewed annually as part of the school's Online Safety Audit and risk assessment.

Training and Awareness:

- Staff receive training on cybersecurity best practices, including phishing awareness, data protection, and secure use of devices.
- Pupils are taught the importance of secure passwords, responsible online behaviour, and how to report suspicious activity.
- The school promotes a culture of cybersecurity awareness across the community.

Incident Response:
In the event of a cybersecurity incident, the school:

- Begin an immediate investigation and where appropriate, containment.
- Notification of affected parties and relevant authorities (e.g., ICO if applicable).
- Review and improvement of systems to prevent recurrence.

19. Effectiveness

To ensure the effectiveness of Pennthorpe's filtering and monitoring systems, the school will audit the filtering system at least once every half term and log results to ensuring its operating as expected.

Implementation:
The Head of Digital Learning, in collaboration with the DSL and Network Manager, will complete an assessment of all filtering, monitoring and security systems annually as below.

The assessment will cover:

- *Role assignment* – clarity on who is responsible for filtering and monitoring.
- *Detection capabilities* – ensuring systems can detect harmful content in real-time or as close to it as possible.
- *Age-appropriate filtering* – ensuring pupils are protected according to their developmental stage.
- *Review cycle* – confirming that filtering and monitoring systems are tested and updated regularly.

Documentation and Reporting:

- Findings from the self-assessment will be documented and shared with the Welfare Committee and Governing Body as part of the school's safeguarding report.
- Any identified gaps or risks will be addressed through updates to systems, staff training, or policy amendments.

Continuous Improvement:

- The school will periodically test its filtering systems using recognised tools (e.g. TestFiltering.com) to ensure they are functioning effectively.
- Logs of filtering changes and incident responses will be maintained and reviewed to inform future improvements.

20. Community Involvement in Audits

Pennthorpe recognises that effective online safety provision benefits from the active involvement of the whole school community. In line with best practice and guidance from Keeping Children Safe in Education (KCSIE) 2025, the school is committed to engaging a broad range of stakeholders in its annual online safety audit and risk assessment process.

Stakeholder Engagement:

The annual online safety audit will include input from:

- Staff across teaching and support roles.
- Governors, particularly those with safeguarding oversight.
- Pupils, through age-appropriate surveys or focus groups.
- Parents and carers, via feedback forms, workshops, or informal consultations.

Implementation:

- The Welfare Committee will coordinate stakeholder involvement and ensure findings are documented and reported to the Governing Body.
- Feedback will be used to inform updates to the Online Safety Policy, staff training, curriculum planning, and parental engagement strategies.

Transparency and Communication:

- A summary of audit findings and planned actions will be shared with stakeholders through newsletters, parent forums, and staff briefings.
- Pupils will be informed of changes to online safety provision through assemblies, PSHE lessons, and digital learning sessions.