The Pennine Trust

Creating opportunity. Inspiring excellence. Shaping tomorrow.

ONLINE SAFETY POLICY

Document Control:

This document has been approved for operation within:	The Pennine Trust		
Status	Statutory		
Owner	The Pennine Trust		
Date effective from	January 2025	**Date of next review**	December 2025
Review period	Annually	**Version**	3

Version	Changes identified
3	• Section 1: Legal framework – in line with recent legislation changes. • Section 3: Roles and responsibilities – some roles updated in line with up to date legislation and contextual knowledge of online risks. • Section 5: Child on Child sexual abuse and harassment – some revision and simplification. • Section 8: Online hoaxes – simplification and focus on current risks • Section 11: Curriculum – role of DSL clarified as advisory, and Appendix A condensed to a list of broad content areas. • Section 13: Use of smart technology - Effectively removed due to use of mobile devices being prohibited during the school day. • Section 17: Network security - Simplified and updated to reflect current cyber-security risks and our approaches to mitigate them. • Section 21: Use of devices - Schools required to insert bespoke summaries of how visitors are informed about expectations re: use of personal devices.

Contents:

Statement of intent

The Pennine Trust understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

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

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

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

1. Legal framework

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE 'Keeping children safe in education' latest version
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Child Protection Policy
- Anti-Bullying Policy

- Relationships and Health Education Policy
- Staff Code of Conduct and Technology Acceptable Use Agreement
- Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Prevent Duty Policy

2. Roles and responsibilities

The Standards Committee (which may delegate some or all of these actions to the CEO) is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at least annually thereafter.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with IT staff and service providers.
- Ensuring that all relevant staff, which includes the SLT in schools, 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.

The Headteacher is responsible for:

- Ensuring vigilance around online safety is a strong feature of the culture of the school and is embedded through policies, systems and procedures, in particular those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date, and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Keeping parents up to date with current online safety issues and how the school is keeping pupils safe.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and IT Manager.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.

- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update procedures.
- Reporting to the LSC about online safety.
- Working with the headteacher and IT Manager to review the effectiveness of this policy on an ongoing basis.
- Working with the CEO and IT Manager to update this policy on an annual basis.

Our IT Manager is responsible for:

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

All staff members are responsible for:

- Taking responsibility for the security of IT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having understanding of online safety issues in line with staff training, including the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- Adhering to the Technology 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.

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

The importance of online safety is integrated across all school operations in the following ways:

- Staff receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum, most notably through the Computing curriculum and the PSHE Education curriculum
- Assemblies are conducted on the topic of remaining safe online

Handling online safety concerns

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 staff member's online behaviour are reported to the headteacher, who will contact the Head of HR to determine the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the Headteacher, it is reported to the CEO.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Headteacher and IT technician, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Child Protection and Safeguarding Policy.

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

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

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

4. Cyberbullying

Cyberbullying can include (but is not limited to) the following:

- Threatening, intimidating or upsetting messages
- Threatening or embarrassing pictures and video clips
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom/group chat
- Unpleasant or defamatory information posted to blogs, personal websites, and social networking sites.

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.

5. Child-on-child sexual abuse and harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this 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 following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child Protection Policy and the Child-on-Child Abuse Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child Protection Policy and Child-on-Child Abuse Policy.

6. Grooming and exploitation

Grooming is defined as the situation whereby a person 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, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that any safeguarding training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are. Signs may include:

- Having unexplained money, gifts and new possessions
- Being secretive about how they're spending their time, including when using online devices
- Sudden changes in behaviour or mood
- Having a friendship or relationship with a much older person
- Spending more time away from or going missing from home or school

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 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. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

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 propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the school's Prevent Duty Policy.

7. 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. Guidance on these issues is included in annual safeguarding training.

8. Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie 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.

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 immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention in line with the guidance in Keeping Children Safe in Education and the DfE's guidance: Harmful online challenges and online hoaxes - GOV.UK.

9. Cyber-crime

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 will consider a referral to the Cyber Choices programme, via the National Crime Agency.

10. Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. 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.

Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy and the Child Protection and Safeguarding Policy.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the Computing curriculum and the Personal, Social, Health and Economic Education curriculum, and in reference to the UKCIS document, 'Education for a Connected World – 2021 edition'.

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. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- What healthy and respectful relationships, including friendships, look like
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform inappropriate or sexual acts
- Acceptable and unacceptable online behaviour
- How and when to seek support
- How to recognise when something they are being asked to do is deceitful, puts them at risk or is age-inappropriate

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix A of this policy.

The DSL is involved with advising on the content of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

The school recognises that, while any pupil can be vulnerable online, 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 Looked After Children. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Senior Leadership and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Pupils who are particularly vulnerable due to previous experiences should be known to staff delivering online safety lessons. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

12. Use of technology in the classroom

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

13. Use of smart technology

Use of personal mobile devices is not permitted during the school day.

14. Educating parents

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

Parents will be made aware of the various ways in which their children may be at risk online and will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

- Newsletters
- 'Advice for Parents' section of the school website
- 'Wellbeing and Safeguarding Support' section of the school website
- Parental meetings

15. Internet access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and acknowledged the Acceptable Use Agreement through The School Bus/Policy Manager.

All members of the school community use the school's internet network, as it has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16. Filtering and monitoring online activity

The Board of Trustees 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 Board of Trustees will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The school uses Netsweeper and Senso filtering and monitoring service.

Requests regarding making changes to the filtering system from staff, such as adding websites that are currently being blocked by the system, should be directed to IT Manager. The IT Manager will take the decision to either add the website to the permittable list or not based on completing a risk assessment as to the content. Netsweeper and Senso provides reports of what is being blocked and who has requested it. Reports of inappropriate websites or materials are made to the trust's ICT team immediately, who then investigates the matter and make any necessary changes.

Deliberate breaches of the filtering system are flagged by Netsweeper and Senso and are reported in real time to the DSL and IT team, who will escalate the matter appropriately. If a pupil or member of staff has breached the filtering system, the matter will be investigated. If the breach is found to be deliberate the pupil or member of staff will be disciplined in line with the relevant policy.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately.

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

17. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by IT technicians. Firewalls will be switched on at all times.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments and are expected to report all malware and virus attacks to IT technicians.

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils are provided with their own unique username and private passwords. Staff members and pupils are responsible for keeping their passwords private.

Users inform IT technicians if they forget their login details, who will arrange for the user to reset their login details. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. Users are required to lock access to devices and systems when they are not in use.

18. Emails

Access to and the use of emails is managed in line with the Data Protection Policy and Acceptable Use Agreement.

Staff and pupils are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and acknowledge the Acceptable Use Agreement through The School Bus. Any email that contains sensitive or personal information should only be sent using secure and encrypted email or be password protected according to the level of security needed.

Staff are given training on how to recognise and report spam and junk mail. The system filters potentially unsafe spam emails; pupils do not receive external emails unless explicitly allowed through the filter. The school's monitoring system can detect inappropriate links, malware and profanity within

emails – staff and pupils are made aware of this. The Computing curriculum and PSHE Education curriculum cover security issues, including the following:

How to determine whether an email address is legitimate

- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails are managed in line with the Data and Cyber Response Plan.

19. Generative artificial intelligence (AI)

Schools 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 ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

See Safe Use of AI Policy.

20. Social networking

Personal use

Access to social networking sites is filtered as appropriate. Staff are not permitted to use social media for personal use during lesson time. Staff can use personal social media during break and lunchtimes; however, staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media in line with KCSiE, the teacher standards and other professional standards – staff members are required to follow these expectations at all times.

Staff receive annual training on how to use social media safely and responsibly. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media. Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are friends with a parent at the school, they will disclose this to the DSL/Headteacher and will adhere to guidance in the Technology and Acceptable Use Agreement.

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

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

Use on behalf of the school

The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the Headteacher to access the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

20. The school website

The Headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website if the provisions in the Data Protection and Records management Policy are met.

21. Use of devices

School-owned devices

Many staff members are issued with a laptop to assist with their work.

Pupils are occasionally provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. laptops to use during lessons.

School-owned devices are used in accordance with the Technology and Acceptable Use Agreement. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected. All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen. All school-owned devices are fitted with software to ensure they can be remotely accessed in case data on the device needs to be protected, retrieved or erased.

All school-owned computers are set to update software automatically. IT technicians will force an update as and when required, such as loading software as part of the general upkeep. No software, apps or other programmes can be downloaded onto a device without authorisation from IT technicians.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behavioural Policy respectively.

Personal devices

Personal devices are used in accordance with the Staff IT and Electronic Devices Policy.
Any personal electronic device that is brought into school is the responsibility of the user.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of pupils.

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

Each school to outline how visitors are informed around expectations of using personal devices.
Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

22. Remote learning

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

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

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

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

23. Monitoring and review

The Standards Committee and DSL review this policy in full on an annual basis and consider amendments following any online safety incidents.

Changes made to this policy are communicated appropriately to relevant members of the school community.

Appendix A: Online harms and risks – expectations of broad areas of curriculum coverage

- Age restrictions
- How content can be used and shared
- Disinformation, misinformation and hoaxes
- Fake websites and scam emails
- Online Fraud
- Password phishing
- Personal data
- Persuasive design
- Privacy settings
- Targeting of online content
- Online abuse
- Challenges
- Content which incites violence
- Fake profiles
- Grooming
- Livestreaming
- Unsafe communication
- Impact on confidence (including body confidence)
- Impact on quality of life, physical and mental health and relationships
- Online vs. offline behaviours
- Suicide, self-harm and eating disorders