

PENWORTHAM GIRLS' HIGH SCHOOL

Online Safety Policy

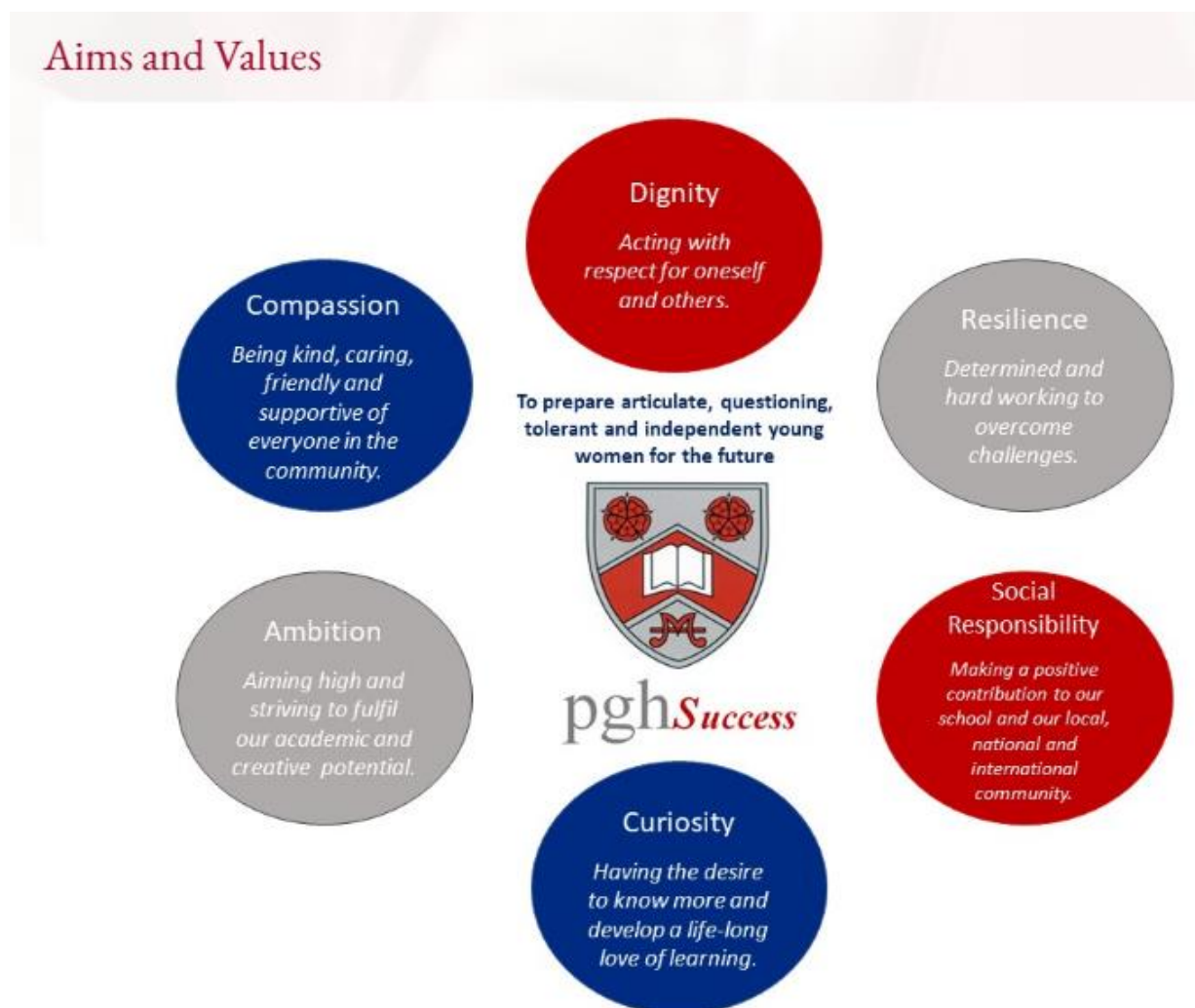
February 2024

**Updated Annually
Next review: Feb 2025**

THE MISSION

**To prepare
articulate, questioning, tolerant and independent women
for the future.**

Aims and Values of the School



Related Policies and documentation:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Computing Scheme of Learning and Resources
- Staff Code of Conduct
- Child on Child Abuse policy

Contents:*Statement of intent*

1. Legal framework
2. Roles and responsibilities
3. Managing online safety
4. Cyberbullying
5. Child on Child sexual abuse and harassment
6. Grooming and exploitation
7. Mental health
8. Online hoaxes and harmful online challenges
9. Cyber-crime
10. Online safety training for staff
11. Online safety and the curriculum
12. Use of technology in the classroom
13. Use of SMART technology
14. Educating parents
15. Internet access
16. Filtering and monitoring online activity
17. Network security
18. Emails
19. Social networking
20. The school website
21. Use of school-owned devices
22. Remote Learning
23. Managing reports of online safety incidents
24. Monitoring and review

Statement of Intent

Penwortham Girls High School understands that using technology is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning. It is also acknowledged that the use of technology and tools such as social media are now an integral part of life outside of school.

It is our intent to create independent, questioning and resilient users of technology. The school is committed to teaching students about the underpinning knowledge and behaviours that will support them in navigating the online world safely and with confidence.

The use of technology is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of students and staff.

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

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **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 students 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 by all students and staff.

1. Legal framework

1.1 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 (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2022) 'Keeping children safe in education 2023'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) '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 (2018) 'Small Business Guide: Cyber Security'

1.2 This policy operates in conjunction with the following school policies:

- Policy on the Use of Social Networking Sites and other forms of Social Media
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement
- Safeguarding Policy
- Anti-Bullying Policy
- Sex and Health Education Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Emotional Health and Well-being Policy
- Child on Child Abuse Policy

2. Roles and responsibilities

2.1 The governing body 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 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 ICT staff and service providers.
- 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 all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

2.2 The headteacher 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 all staff undergo safeguarding and child protection training (including online safety) at induction.
- Supporting the DSL and any deputies 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 students can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping students safe.
- Working with the DSL and ICT manager to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.

2.3 The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.

- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that students with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCo and ICT 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.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that 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.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Working with the headteacher and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on an annual basis.

2.4 The ICT 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.
- Working with the DSL and headteacher to conduct half-termly light-touch reviews of this policy.

2.5 All staff members are responsible for:

- Taking responsibility for the security of ICT 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 an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that students 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.
- Ensuring that Impero Confide is used to monitor students when using technology in the classroom.

2.6 Students are responsible for:

- Adhering to this policy, the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has 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 the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about students' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

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

- Staff and governors 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
- Assemblies are conducted regularly on the topic of remaining safe online

Handling online safety concerns

Any disclosures made by students 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 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, and Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a student's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature.

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

The school avoids unnecessarily criminalising pupils. 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 on cpoms.

4. Cyberbullying

Cyberbullying can include the following:

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- 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
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

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

Students may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that students 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
- 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-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-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

6. 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 students who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The student 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 student 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 student 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 student feel 'special', particularly if the person they are talking to is older.
- The student 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 students 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 online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

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 student may be groomed online to become involved in a wider network of exploitation, e.g. the production of abusive sexual images of children, coerced child sexual activity 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 students 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 students at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any students displaying indicators that they have been, or are being, radicalised.

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

7. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in students, 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 student's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet, in general, can impact mental health, and the indicators that a student is suffering from challenges in their mental health. Concerns about the mental health of a student will be dealt with in line with the Emotional Health and Wellbeing policy.

8. 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 student 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 students 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, establishing the scale and nature of the possible risk to students, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing students.
- Not inadvertently encouraging students to view the hoax or challenge where they would not have otherwise come across it
- Proportional to the actual or perceived risk.
- Helpful to the students who are, or are perceived to be, at risk.
- Appropriate for the relevant students' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting students at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting the potential harms of a hoax or challenge when the risk of needlessly increasing students' exposure to the risk is considered and mitigated as far as possible.

9. 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 students 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 student's use of technology this matter will be referred to the DSL.

The DSL and headteacher will ensure that students are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that students cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology.

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, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems.

All staff will be made aware that students 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 following subjects:

- Life Skills curriculum (RSE, Health Education, PSHE and Citizenship)
- Computing

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
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks students may face online are always considered when developing the curriculum. Students 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 DSL is involved with the development of the school's online safety curriculum.

The school recognises that, while any student can be vulnerable online, there are some students who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. students with SEND and LAC. Relevant members of staff, e.g. the SENCo and designated teacher for LAC, work together to ensure the curriculum is tailored so these students 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 students.

Curriculum leaders review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of students.

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

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that students in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any student who may be especially impacted by a lesson or activity.

Lessons and activities are planned carefully so they do not draw attention to a student who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which students feel comfortable to say what they feel and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything students raise or disclose during online safety lessons and activities, they will use the normal school safeguarding protocols and record the concern on cpoms.

12. Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets

- Email
- Cameras

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.

Students are supervised when using online materials during lesson time using the Impero system.

13. Use of SMART technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Students will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Technology Acceptable Use Agreement for Students.

Staff will use all smart technology and personal technology in line with the school's Staff ICT and Electronic Devices Policy.

The school recognises that students' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Students will not be permitted to use smart devices or any other personal technology whilst in the classroom.

Where it is deemed necessary, the school will ban students's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among students, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating parents

The school works in partnership with parents to ensure students 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 the Acceptable Use Agreement at the beginning of each academic 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 will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents 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:

- Parents' evenings
- Newsletters
- The safeguarding section of the school website

15. Internet access

Students, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

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

16. Filtering and monitoring online activity

The 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 school's and colleges'. The governing board 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 headteacher and ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are appropriate to students' ages, the number of students using the network, how often students access the network, and the proportionality of costs compared to the risks. ICT technicians undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL conduct a risk assessment. Any changes made to the system are recorded by ICT technicians. Reports of inappropriate websites or materials are made to the ICT manager immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and the ICT manager, who will escalate the matter appropriately. If a student has deliberately breached the filtering system, they will be disciplined in line with the Behavioural Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

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.

Generative artificial intelligence (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 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 ensure that pupils are not accessing or creating harmful or inappropriate content, including 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.

17. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by the ICT manager. Firewalls are switched on at all times. The ICT manager review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and students are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to the ICT manager.

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

Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different 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 will be managed in line with the Data Protection Policy and the Acceptable Use Agreement.

Staff and students will be given approved school email accounts and will only be 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 students must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and students will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and students will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

19. Social networking

Personal use

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 – 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 students or parents over social networking sites and are reminded to alter their privacy settings to ensure students and parents are not able to contact them on social media.

Where staff have an existing personal relationship with a parent or student 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 and headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

Students 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 Behaviour Policy.

Use on behalf of the school

The school's official social media channels are only used for official educational or engagement purposes.

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 students is not published on the website. Images and videos are only posted on the website if appropriate permissions are granted.

21. Use of school-owned devices

Use of personal devices

Any personal electronic device that is brought into school is the responsibility of the user.

Personal devices are not permitted to be used in the following locations:

- Toilets
- Changing rooms

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 students.

Staff members report concerns about their colleagues' use of personal devices on the school premises to the headteacher. 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.

Students are not permitted to use their personal devices during the school day and all devices should be stored in their locker. If a student needs to contact their parents during the school day, they are allowed to use the phone in the school office. The headteacher may authorise the use of mobile devices by a student for safety or precautionary use.

Students' devices can be searched, screened and confiscated in accordance with the DFE Searching, screening and confiscation document (2018). If a staff member reasonably believes a student's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

22. Remote learning

All remote learning is delivered in line with the school's Student Remote Learning Acceptable Use Policy.

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.

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.

23. Managing reports of online safety incidents

Staff members and students are informed about what constitutes inappropriate online behaviour in the following ways:

- CPD sessions
- The online safety curriculum
- Assemblies

Concerns regarding a staff member's online behaviour are reported to the headteacher who decides on the best course of action in line with the relevant policies.

Concerns regarding a student's online behaviour are reported to the DSL who investigates concerns with relevant staff members, e.g. the headteacher and the ICT manager.

Concerns regarding a student's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. Behaviour Policy and the Safeguarding Policy.

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

24. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT manager and the headteacher conduct half-termly light-touch reviews of this policy to evaluate its effectiveness.

The governing body, headteacher and DSL review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is February 2025.

Any changes made to this policy are communicated to all members.

This policy has been agreed by the Governing Body	DATE
Reviewed – Curriculum & Standards (known as E Safety Policy)	February 2018
Reviewed – Curriculum & Standards (known as E Safety Policy)	February 2019
Reviewed – Curriculum & Standards (known as E Safety Policy)	February 2020
Reviewed – Curriculum & Standards	February 2021
Reviewed – Curriculum & Standards	February 2022
Reviewed – Curriculum & Standards	February 2023
Reviewed – Curriculum & Standards	February 2024

