Penwortham Priory ACADEMY

Online Safety Policy

Prepared/Updated :	August 2025
Review Frequency :	Every year or as required by DfE
Next Review Due :	August 2026

Contents

Statement of intent

Penwortham Priory Academy 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, for example:
  - Pornography.
  - Racism.
  - Misogyny.
  - Self-harm.
  - Suicide.
  - Discrimination.
  - Radicalisation.
  - Extremism.
  - Misinformation.
  - Disinformation, including fake news.
  - Conspiracy theories.

- **Contact**: Being subjected to harmful online interaction with other users, for example:
  - Peer to peer pressure.
  - Commercial advertising.
  - Adults posing as children or young adults with the intention to groom or exploit children 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 messages.
  - Consensual and non-consensual sharing of nudes and semi-nudes.
  - Sharing of pornography.
  - Sharing other explicit images.
  - Online bullying.

- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff will revolve around these areas of risk. Penwortham Priory Academy 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.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of our wider duty of care to which all who work in schools are bound. The school online policy will help to ensure safe and appropriate use. The development and implementation of this policy will involve all of the stakeholders in a child's educations from the Principal and Trustees to SLT and classroom teachers, support staff, parents and pupils themselves. Penwortham Priory Academy have robust safeguarding procedures in place and understands that online safety is an integral part of keeping children safe.

The use of these exciting and innovative technologies and tools in school and at home has been shown to raise educational standards and promote pupils achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers may include :-

- Access to illegal, harmful or inappropriate images or content
- Unauthorized access to / loss of / sharing of personal information
- The risk of subject to grooming by those with whom they have contact on the internet
- The sharing / distribution of personal images without an individuals consent or knowledge.
- Inappropriate communication / contact with others, including strangers
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential of excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situation in the off-line world and it is essential that this online safety policy us used in conjunction with other school policies (eg. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential through good education provision to build pupils' resilience and raise awareness of the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school will demonstrate that it has provided the necessary safeguarding to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online safety policy that follows explains how we at Penwortham Priory Academy intend to do this, whilst also addressing wider educational issues in order to help young people to be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.

Online safety encompasses not only internet technologies but also electronic communications via mobile phones games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- Online safety concerns safeguarding children and young people in the digital world
- Online safety emphasizes learning to understand and use new technologies in a positive

way

- Online safety is less about restriction and more about education and risks as well as the benefits so we can feel confident online
- Online safety is concerned with supporting children and young people develop safer online behaviours both in and out of school

The internet is an unmanaged, open communications channel. The World Wide Web, emails, blogs and social networks all transmit information using the internet intentionally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the internet make it an invaluable resources used by billions of people every day.

Some of the material on the internet is published for an adult audience and can include violent and adult content. Information on weapons, crime, racism, extremism and radicalization may also be unsuitable for children and young people to access. Pupils need to develop critical skills to evaluate online material and learnt that publishing personal information could compromise their security an that of others. Schools have a duty of care to enable pupils to use online systems safely.

Penwortham Priory Academy needs to protect itself from legal challenge and ensure that staff work within boundaries of professional behaviour. The law is catching up with internet developments: for example it is an offence to use email, text or instant messaging (IM) to 'groom' children.

It is the responsibility of the school to make it clear to staff, pupils and visitors that the use of school equipment for inappropriate reasons is 'unauthorised' and an acceptable use policy (AUP) is in place. Online safety training is and essential part of staff induction, continued INSET and part of our ongoing CPD programme.

IT System

- Schools firewalls are Fortigate 90G and operate 2 of these in a failover state. Our filtering is provided by Lightspeed Systems. On all school owned devices, Lightspeed filtering client installed and on pupil devices Lightspeed Alerting client has been installed
- Both the Fortigate & Lightspeed conform to the IWF and CTIRU lists of blocked websites and updates the systems accordingly.
- All staff and pupils sign the School Acceptable Use Agreement for use of computers in school.

The rapid development and accessibility of the internet and new technologies such as personal phishing and social networking, means that online safety is an ever growing and changing area of interest and concern. The school's online safety policy reflects this by keeping abreast of the vast changes taking place around us.

Please note : school devices will only be monitored in school work hours.

In the event of a cyberattack, the school will revert to its cyber risk policy.

This policy applies to all members of the school community which have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers and Principals to such extent as it is reasonable, to regulate behaviours of pupils when they are off the school site and empowers members of staff to impose sanctions for inappropriate behaviours. This is pertinent to online bullying, which may take place out of school, but is linked to membership / belonging to the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents, guardians and / or carers of incidents of inappropriate online behaviour that take place out of school.

The school will monitor the impact of the policy using :

- Internal monitoring data for network activity
- Internet monitoring which is done by schools own Lightspeed System & Filter
- Lead DSL logs on incidents
- Monitoring logs of internet activity, including sites visited
- Lightspeed safeguarding alerts sent to DSLs
- the IT team who will work to ensure filtering systems are appropriate, efficient and as effective as possible. This will entail regularchecks and ongoing monitoring.
- Lightspeed Systems with the appropriate firewall and all appropriate filters.
- virus protection that will be regularly updated. There should be procedures in place for virus protection to be updated on any laptops used by staff members or pupils.

If staff or pupils discover unsuitable sites, the URL, time and date must be reported immediately to the network manager. There are processes in place to deal with such reports

Aims

At Penwortham Priory Academy, we are committed to using the internet and other digital technologies to:

- Make learning more exciting and interactive.
- Make lessons more varied.
- Enable pupils to gain access to a wide variety of knowledge in a safeway.
- Raise educational standards.
- Prepare our pupils for using the internet safely outside of school and throughout their education

Definition

Online safety encompasses a number of technologies such as computers, tablet computers, internet technologies and any other mobile device

Online safety measures

Penwortham Priory Academy's internet systems, and access to it, is specifically designed for staff and pupil use, as such, includes filtering appropriate for ages.

Pupils will have clear objectives about why they are using the internet whenever the internet is incorporated into lessons.

Lessons using the internet will be carefully planned and the 'access levels' classes and pupils are afforded will be fully considered, taking into account pupil age and curriculum requirements. Children using the internet will do so in classrooms (or other appropriateshared areas of the school) during lesson time only and with teacher supervision.

Pupils will be taught what internet use is acceptable and unacceptable,and teachers should be vigilant during internet-based lessons.

Particular vigilance is necessary if and when pupils are undertaking internet searching. Teachers should use their professional judgement regarding whether this internet function is appropriate for the relevantclass.

If the Google images website is used in class, this should be done usingthe 'safe search' function. Teachers can make judgement calls on whether to allow the use of Google images at all, due to the range of content and possibility for accessing inappropriate material. Records will be maintained detailing all staff and pupils who have internet access.

Legal framework

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

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2025) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2025) 'Keeping children safe in education 2025' (KCSIE)
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2025) '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 (updated March 2024)'
- 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:

- Social Media Policy
- Allegations of Abuse Against Staff Policy

- Acceptable Use Agreement
- Cyber Response and Recovery Plan
- Child Protection and Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Staff Code of Conduct Policy
- Behaviour and Discipline Policy
- General Data Protection Regulations Policy
- Photography and Videos at School Policy
- Prevent Duty Policy
- Use of Artificial Intelligence Policy

Roles and responsibilities

The ***Chair of Trustee / Safeguarding Trustee*** will be 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 regular intervals.
- 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.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.

At Penwortham Priory Academy, The Chair of Trustee / Safeguarding Trustee is Dr Range.

The ***Principal and SLT*** will be 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.

- 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.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT Support team to conduct halt-termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.
- Identifying and assigning roles and responsibilities to manage the school's filtering and monitoring systems.
- Appointing an SLT digital lead in line with the Cyber-security requirements / policy

The ***DSL*** will be 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 ICT Support team.
- 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.
- Providing specialist knowledge in relation to filtering system management, e.g. the content and websites pupils should and should not be able to access.
- 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.
- 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 trustee board about online safety on a termly basis.
- Working with the Principal and ICT Support team to conduct half-termly light-touch reviews of this policy.

- Working with the Principal and trustee board to update this policy on an annual basis.

At Penwortham Priory Academy, Lead DSL is Mrs Crank (Assistant Principal) and DSLs are Mrs Holland and Mr Faulkner.

ICT Support team will be 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 Principal.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and Principal to conduct half-termly light-touch reviews of this policy.
- Providing specialist support in relation to the implementation of filtering and monitoring software.

All staff members will be 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 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 will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

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 Principal where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' 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 trustees 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 termly on the topic of remaining safe online

At Penwortham Priory Academy, DSL responsible for Online Safety is Mrs Crank (Assistant Principal).

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.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the Principal, who decides on the best course of action in line with the relevant policies. If the concern is about the Principal, it is reported to the Chair of Trustees.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Principal and ICT Support team, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour and Discipline Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Principal or DSL will contact 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.

Cyberbullying

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.

Child-on-child sexual abuse and harassment

Pupils 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, 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.
Penwortham Priory Academy 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 and the Social Media Policy.

Penwortham Priory Academy 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.

Grooming and exploitation
Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.
Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. 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 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 online.
- 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 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 Prevent Duty Policy.

Mental health

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. 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 pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an "**online hoax**" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, "**harmful online challenges**" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL 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 pupils, 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 Principal 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 pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' 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 pupils at risk of harm, 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 individual pupils at risk where appropriate.

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

Cyber-crime

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

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

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

The DSL and Principal will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

Online safety training for staff

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

Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSHE
- PSHE
- Citizenship
- ICT & Technology

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 pupils may face online will always be considered when developing the curriculum. Penwortham Priory Academy's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

Content Risks
Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. The curriculum will include discussions around harmful content such as pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.

Contact Risks
The school will educate pupils about the potential dangers of interacting with others online. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

Conduct Risks
Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with creating, sharing, or receiving explicit images, including both consensual and non-consensual exchanges of nudes and semi-nudes. Online bullying, including the use of social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce Risks
The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when confronted with suspicious online activity.

The DSL will be involved with the development 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.

Relevant members of staff, e.g. the SENCO and designated teacher for children looked after (CLA), will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and CLA, receive the information and support they need.

At Penwortham Priory Academy, the SENCO is Mrs Holland.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

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 Principal and DSL will 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 will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. 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.

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

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.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Use of technology in the classroom

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

- Computers
- Laptops
- Email
- TEAMs

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 will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

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

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.

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

Staff will use all technology and personal technology in line with the school's Acceptable Use Agreement for Staff.

Penwortham Priory Academy recognises that pupils' 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.

Pupils 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 pupil's use of personal technology whilst on school site. Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour and Discipline 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.

Education & Training

Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online safety training will be made available to staff.

- Staff are familiar with the guidance related to Online Safety in Keeping Children Safe in Education 2025
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies
- The Online Safety Designated person will receive regular updates from the Lead of Computing / Network managers / ICT Team through attendance at LA / other information / training sessions and by reviewing guidance documents released by the local authority and others.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Online Safety Designated person will organise the provision of advice / guidance / training to individuals as required

Staff Training

- All staff and pupils to receive regular and up-to-date training via PSHE, LfL, Computing and within departments for pupils. INSET provision will be provided for school-based staff.
- Pupils will receive age appropriate online safety information within the school curriculum which focusses on how to stay safe, protect themselves from harm and how to take responsibility for their own online safety and that of others.

Trustees

- Trustees should take part in online safety training / awareness sessions, with particular importance for those who are members of any committee / group involved in ICT / online safety / health and safety / child protection. This may be offered in a number of ways:
    - Attendance at training provided by the Local Authority / National Governors Association or other relevant organisations.

Parents and carers

Penwortham Priory Academy will work in partnership with parents and carers to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents sign the Acceptable Use Agreement when their child is admitted to Penwortham Priory Academy. Pupils are reminded of this during lessons and assemblies and children understand the document and the implications of not following it.

Parents and carers 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 and carers 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 will be raised in the following ways:

- Parents' evenings
- Newsletters
- Monthly safeguarding newsletters
- Online resources
- Online Safety page on the academy's website

Communications

The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore be encouraged to use only the school email service to communicate with others in school, or on school systems, such as TEAMs.

- Users need to be made aware that email communications may be monitored
- Users must immediately report, to the nominated person, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat TEAMs etc) must be professional in tone and content. These communications should only take place on official school systems. Personal email address, text messaging or public chat / social networking programmes must **not** be used for these communications.
- Pupils will be provided with individual school email addresses for educational use
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material / language.
- Personal information should not be posted on the school website and only official email address should be used to identify members of staff.
- Pupils should be taught not to reveal personal details about themselves or others in email or digital communication. This will generally include full names, addresses, mobile or landline phone numbers, school name, instant messenger (IM)address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils should never to arrange to meet someone they have 'met' via e-mail/online without appropriate safeguarding measures (e.g. the presence of a parent or

responsible adult).

Parents and pupils alike should both be informed of the risks inherent in using social media. Social media websites will not be accessible throughthe school's network and should not be accessed on school devices through other networks.

Whenever staff or pupils send e-mails to organisations or persons outside of the school, these should be authorised in the same wayofficial school correspondence would be.

Use of digital and video images – photographic, video etc

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.

However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm :

- When using digital images, staff should inform and educate pupils about the risk associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognize the risks attached to publishing their own images on the internet eg. on social networking sites
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of these images. Those must be taken on school equipment.
- The personal equipment of staff should only be used for such purposes when school equipment is not available and there is a clear educational benefit to taking a digital / video image.
- Digital images / video should be removed or deleted from the equipment as soon as possible and should only be stored on school equipment and for minimum period of time necessary.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individual or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others
- Photographs published on the website, or elsewhere that include pupils will comply with good practice on the use of such images
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Consent from parents / carers is obtained before photographs of pupils are taken or are

published on the website. This consent can be located in the data collection booklets that parents complete when their child starts at school.

Data Protection Personal Data

Data Protection Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimizing the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Request a DP1 form when submitting names and contact details to the Police.

When personal data is stored on any portable computer system:

- The data must be encrypted and password protected.
- The device must be password protected.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.
- The device must offer approved virus and malware checking software

Web-based technologies

- The Internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available.
- Use of email enables improved communication and facilitates the sharing of data and resources.

- Virtual Learning Environments (VLEs) provide pupils with a platform for personalised and independent learning.

Risks

- Pupils might inadvertently access content of an unsavoury, distressing or offensive nature on the Internet or receive inappropriate or distasteful e-mails.
- Pupils might receive unwanted or inappropriate e-mails from unknown senders, or be exposed to abuse, harassment or online bullying via e-mail, text or instant messaging, in chat rooms or on social-networking websites and apps, such as Facebook, Whatsapp, Instagram etc.
- Chat rooms provide cover for unscrupulous individuals to groom children

Procedures for use of a shared network

- Users must access the network using their own accounts. These must not be disclosed or shared.
- Users must respect confidentiality and attempts should not be made to access another individual's account or files on the network without permission of the Principal.
- Software should only be installed by the ICT Support Team at Penwortham Priory Academy.
- Users must ensure they have adequate virus protection on any device on which they access school resources.
- Computers, laptops etc … must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.'
- All computer screens in school also have an automatic lock on after a period of time of non-use.
- Laptops, computers etc … must be 'logged off' correctly after use.

Procedures for use of the internet and email

- All users must sign an 'Acceptable Use Agreement' before access to the Internet and email is permitted in the establishment.
- Users must access the Internet and e-mail using their own account and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's e-mail account. If you feel your account details are known by others you should change your password immediately.
- The Internet and e-mail must be used in a reasonable manner adhering to the professional judgment of the supervising member of school staff.
- Pupils must be supervised at all times when using the Internet and e-mail in school. During lessons, pupils will always be reminded that everything on the school network is monitored
- Procedures for safe Internet use and sanctions are applicable if rules are broken.
- Internet and e-mail filtering software is installed to restrict access, as far as possible to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted

correspondence. This is to be reviewed and updated regularly.

- Internet and e-mail use will be monitored regularly in accordance with the Data Protection Act 2018.
- Users must be careful when they disclose any information of a personal nature in an e-mail or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.
- All e-mails sent should be courteous and the formality and tone of the language used appropriate to the reader. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- Bullying, harassment or abuse of any kind via e-mail will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- If users are bullied, or offensive e-mails are received, this must be reported immediately to a trusted adult or member of staff within Priory. Emails received should not be deleted, but kept for investigation purposes.
- Copyright must not be broken.

File transfer:

- Files may be taken home or brought into school by staff and pupils by using **One Drive**.
- Remember - the school uses special filtering software, which prevents you from accessing most unsuitable sites and it also records every attempt you make to hit a site, whether successful or not, when and where you did it and who you are.
- So remember - every action you take under your account is recorded, and may be accompanied by screenshots and/or recordings of your session.

Unsuitable / Inappropriate Activities
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

The school policy restricts certain internet usage as follows :

Procedures for use of cameras, digital photos, online cameras / devices and any other digital device

- Permission must be obtained from a pupil’s parent, guardian or carer before photographs or video footage can be taken.
- Photographs and/or video footage can be downloaded and stored into an appropriate area under the guidance of the Network Manager. • Any photographs or video footage stored, must be deleted immediately once no longer needed.
- Pupils and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

Procedures to ensure safety of Penwortham Priory Academy website

- All content and images must be approved before being uploaded onto the website prior to it being published.
- The website is checked every term to ensure that no material has been inadvertently posted, which might put pupils or staff at risk.
- Copyright and intellectual property rights are respected.
- Permission is obtained via the data collection sheet from parents, guardians or carers before any images of pupils can be uploaded onto the website.
- When photographs to be used on the website are saved, names of individuals should not be used as file names.

Internet access

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

Filtering and monitoring online activity

The trustee board 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 trustee 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 academy's safeguarding needs.
The Principal and ICT Support team will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems will be scaled appropriately to meet the safeguarding needs of all pupils. ICT Support team will undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the Principal. Reports of inappropriate websites or materials will be made to DSL immediately, who will investigate the matter, inform ICT Support team and collectively makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT Support team, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour and Discipline Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary and Dismissal Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The academy's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored.

Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

All staff will receive regular training on the operation and purpose of filtering and monitoring systems, including their role in safeguarding.

Personal devices connected to the school's network will be subject to the same filtering and monitoring standards to ensure consistent safeguarding measures.

Filtering and monitoring systems will undergo at least an annual review to assess their effectiveness and relevance.

Network security and IT System

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT Support team. Our firewalls are Fortigate 90G and we operate 2 of these in a failover state. Our filtering is provided by Lightspeed Systems.

On all school owned devices, we will have Lightspeed filtering client installed and on pupil devices we will also install the Lightspeed Alerting client. This client will generate alerts if a pupil types in Word, Teams or saves a file in OneDrive that meets the criteria that has been set for key words to trigger alerts to Pastoral staff. These alerts will then need to acknowledge in the software by a member of staff to identify as a concern or a false positive.

Both the Fortigate & Lightspeed conform to the IWF and CTIRU lists of blocked websites and updates the systems accordingly. We also internally use NetSupport Classroom Cloud which monitors keystrokes against a database of known keywords and phrases.

All staff & students sign the School Acceptable Use Agreement for use of computers in school
In the event of needing to switch off the filtering for any reason, or for any user or device, this must be logged and carried outby a process that is agreed by the Principal (or other nominated senior leader). Other aspects of IT system include :

- Any filtering issues should be reported immediately to ICT Support Team.
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Support Team and Strategic Estates Development Manager and / or Principal
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Behaviour Policy.
- Remote management tools are used by staff to control workstations and view user's activity. They will not be used on staff laptops/workstations without prior permission of the staff user.
- Users can report any actual / potential online safety incident to the ICT Support Team
- Curriculum Leader for Business & Computing or Designated Safeguarding Leader in charge of Child Protection. The incident will be reviewed and an appropriate sanction put in place.

- Security measures provided by Fortigate are in place to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- For the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system the ICT Support Team will supply a username and password, and all "guests" will be allowed to use the guest Wi-Fi.
- The downloading of executable files by users is blocked by ICT Support Team.
- Staff are not permitted any personal use on laptops and other portable devices that may be used out of school that belong to school.
- Staff can contact ICT Support Team so that they can install programmes on school workstations / portable devices that they require. This action would be carried out by an IT Technician.
- Agreed guidelines are in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices this type of media is no longer allowed on any school own devices with the exception of the Exams Officer & the ICT Support Team.

The school infrastructure and individual workstations are protected by up to date anti-virus software provided by Microsoft using their Defender product.

All staff Microsoft accounts are protected using MFA and requires the use of Microsoft Authenticator to access accounts online. Staff laptops are registered with Microsoft Windows Hello to allow staff to log into their laptop using facial recognition, pin code or password.

Conditional access policies are also in place so that access is only granted to online Microsoft resources if you are access these from the UK. All other countries are blocked. This policy applies to both staff and students.

Users will inform ICT Support team if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Principal will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use. The SLT digital lead will be responsible for implementing appropriate network security measures in liaison with the DPO and DSL.

The rapid development and accessibility of the internet and new technologies such as personal phishing and social networking, means that online safety is an ever growing and changing area of interest and concern. The school's online safety policy reflects this by keeping abreast of the vast changes taking place around us.

Please note : school devices will ***only*** be monitored in school work hours.

In the event of a cyberattack, the school will revert to its cyber risk policy. This policy applies to all members of the school community which have access to and are users of school ICT systems, both in and out of school

The Education and Inspections Act 2006 empowers Headteachers and Principals to such extent as it is reasonable, to regulate behaviours of pupils when they are off the school site and empowers members of staff to impose sanctions for inappropriate behaviours. This is pertinent to online bullying, which may take place out of school, but is linked to membership / belonging to the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents, guardians and / or carers of incidents of inappropriate online behaviour that take place out of school.

The school will monitor the impact of the policy using :

- Internal monitoring data for network activity
- Internet monitoring which is done by schools own Lightspeed System & Filter
- Lead DSL logs on incidents
- Monitoring logs of internet activity, including sites visited
- Lightspeed alerts sent to DSLs
- the IT Support team who will work to ensure filtering systems are appropriate, efficient and as effective as possible. This will entail regularchecks and ongoing monitoring.
- Lightspeed Systems with the appropriate firewall and all appropriate filters.
- virus protection that will be regularly updated. There should be procedures in place for virus protection to be updated on any laptops used by staff members or pupils.

If staff or pupils discover unsuitable sites, the URL, time and date must be reported immediately to the IT Support team. There are processes in place to deal with such reports.

Emails

Access to and the use of emails will be managed in line with the General Data Protection Regulations Policy and Acceptable Use Agreement.

Staff and pupils 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 pupils 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 pupils will be required to block spam and junk mail, and report the matter to ICT Support team. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this.

As part of online safety programme, pupils will have explained to them what a phishing email and other malicious emails might look like – this assembly will include information on, but not limited to, 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 will be managed in line with the Cyber Response and Recovery Plan.

Generative Artificial Intelligence (AI)

When deciding whether to use generative AI, safety will be the top priority. Any use of AI tools by staff and pupils will be carefully considered and assessed, evaluating the benefits and risks of its use in the school.

AI tools will only be used in situations where there are specified clear benefits that outweigh the risks, e.g. where it can reduce teacher workload, and the school will ensure that any use of AI tools comply with wider statutory obligations, including those outlined in KCSIE.

Pupils will only be permitted to use generative AI in the school with appropriate safeguards in place. Penwortham Priory Academy is committed to prioritising the safety and security of all users when implementing AI systems.

For any use of AI, the school will:

- Comply with age restrictions set by AI tools and open access large language models (LLMs).
- Consider online safety, including AI, when creating and implementing the school's approach to safeguarding and related policies and procedures.
- Consult KCSIE to ensure all statutory safeguarding obligations and AI tools are used safely and appropriately.
- Refer to the DfE's generative AI product safety expectations and filtering and monitoring standards.

Penwortham Priory Academy 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.
- ensure its IT system includes appropriate filtering and monitoring systems to limit pupils' ability to access or create harmful or inappropriate content through generative AI.
- ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.
- take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.
- 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.

Penwortham Priory Academy also has a comprehensive '***Responsible Use of Artificial Intelligence Policy***' that clearly defines how AI technologies will be utilised responsibly and securely. This policy outlines roles including, but not limited to :

- implementation guidelines
- AI in Teaching and Learning
- Roles and responsibilities
- Data protection and Intellectual Property
- Safeguarding Considerations

Social networking
The use of social media by staff and pupils will be managed in line with the academy's Social Media Policy.

Unsuitable / Inappropriate Activities
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows :

Procedures for use of cameras, digital photos, online cameras / devices and any other digital device
Permission must be obtained from a pupil's parent, guardian or carer before photographs or video footage can be taken. Photographs and/or video footage can be downloaded and stored into an appropriate area under the guidance of the Network Manager. Any photographs or video footage stored, must be deleted immediately once no longer needed.

Pupils and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

Procedures to ensure safety of Penwortham Priory Academy website

- All content and images must be approved before being uploaded onto the website prior to it being published.
- The website is checked every term to ensure that no material has been inadvertently posted, which might put pupils or staff at risk.
- Copyright and intellectual property rights are respected.
- Permission is obtained via the data collection sheet from parents, guardians or carers before any images of pupils can be uploaded onto the website.
- When photographs to be used on the website are saved, names of individuals should not be used as file names.

Procedures for using mobile phones, digital and other devices

- The school is **NOT** responsible for pupils' personal mobile technology damaged, lost or stolen. Items are brought to school at your own risk.

- If a mobile phone needs to be brought into school, it should be ***'off and out of sight'*** at all times and stored in bags. They are not to be accessed between entering the school site and 3.10pm.
- If a mobile phone or another device is activated in school it will be confiscated immediately, recorded and handed in to the pastoral office. Pupils will then be able to collect their phones at 3.10pm from a member of the pastoral team. If any pupils repeatedly has their phone taken off them, then parents, guardians will be contacted to discuss this further.
- Staff will not copy/distribute/view images on any pupils' personal mobile device.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Online terrorist and extremist material.
- Other criminal conduct, activity or materials.

If a pupil breaks **any** of the rules, consequences could be:

- A temporary ban on the use of all computer facilities at school until a discussion takes place with the Online Safety Designated Lead, SLT, Lead of Computing and/or a member of the pastoral team
- A ban, temporary or permanent, on the use of the internet facilities at school.
- Appropriate punishment within the departmental and/or school pastoral systems.
- A phone call / letter informing parents what has occurred.
- Referral to Channel, part of Prevent strategy.
- Any other action decided by the Principal and Trustees of the school.
- The flow chart in **Appendix 1** should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Schedule for Monitoring / Review

This online safety policy was approved by SLT	July 2025 and will be updated as and when required.
The implementation of this online safety policy will be monitored by	SLT
Monitoring will take place at regular intervals	Annually
The Trustees will receive a report within the Principal's Termly report on the online safety policy generated by DSLs and pastoral team at Priory. This will include anonymous details of any online safety incidents at regular intervals	Termly
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments (such as Online Safety Bill), and those new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated date will be :	July 2026, in readiness for the new term, September 2026
Serious online safety incidents take place, the following external persons / agencies should be informed :	Lancashire Safeguarding Children Board (LADO) 01772 536694 Lado.admin@lancashire.gov.uk

Concluding statement:
The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology at Penwortham Priory Academy.

It may be that staff / pupils might wish to use an emerging technology for which there are currently no procedures in place. The use of emerging technologies will be permitted upon completion and approval the Principal, SLT and discussions within the IT Support team, which will be used to inform future policy updates.

Appendix 1

Online Incident
Involving pupils at Penwortham Priory Academy

Member of staff assesses severity according to Penwortham Priory Academy's Behaviour and Discipline Policy then :

Low Severity

For example :

- misuse of school email
- off task on the internet

Member of staff follows procedures from Priory's Behaviour and Discipline Policy

Logs incident on Arbor

Medium Severity

For example :

- inappropriate sites
- bypass filters
- playing games

Online Safety Lead receives alert through ClassCloud / Lightspeed – follow procedures from Priory's Behaviour & Discipline Policy.

Incident directly reported to Online Safety Lead / DSL / Pastoral managers – follow procedures from Priory's Behaviour and Discipline Policy

Discussion with child / children. Parents, guardians or carers informed.

Appropriate course of action is determined.

This could include :

account and / or internet may be disabled for period of time.

Supplementary user agreement possibly issued (if req'd) pupil to sign

Log incident on Arbor and CPOMs

High Severity

For example :

- abuse to staff
- misuse of school email system for bullying, child-on-child abuse, cyberbullying, inappropriate images

Report to Network Manager, Online Safety Lead, DSL, Pastoral managers who will discuss with Principal.

Online Safety Lead receives alert through ClassCloud / LightSpeed – follow procedures from Priory's Behaviour and Discipline Policy.

Principal and DSL to decide appropriate course of action.

Account disabled until further notice.

Discussion with child / children. Meeting with parents, guardians or carers.

May be necessary to report to other agencies such as police, children's social care etc …

Log incident on Arbor and on CPOMs

Any online incidents involving a member of staff are reported to The Principal directly who will decide appropriate course of action.

Appendix 2 - Overview of User Actions

		Acceptable	Acceptable at certain times	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data, transfer, communicate or pass on, material, remarks, proposals or comments that contains or relate to :	Child sexual abuse images			X	X
	Promotion or conduct of illegal acts, eg. under the child protection, obscenity, computer misuse and fraud legislation			X	X
	Adult material that potentially breaches the Obscene Act in the UK			X	X
	Criminally racist material			X	X
	Pornography			X	X
	Promotion of any kind of discrimination			X	
	Promotion of any kind of racial or religious hatred			X	
	Threatening behaviour, including the promotion of physical violence / mental harm			X	
	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			X	
Using school systems to run a private business				X	
Use systems, applications, websites or other mechanisms that by pass the filtering or other safeguards employed by the school				X	
Uploading downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				X	
Revealing or publicizing confidential information (eg. personal, financial, databases, computer / network passwords or codes)				X	
Creating / propagating computer viruses or other harmful files				X	

The school website

The Principal has overall responsibility for the content of the school website. This includes ensuring all content is appropriate and accurate. There are procedures in place for authorizing the uploading of any content onto the school's website.

No personal information or contact details will be published on the school's website. This extends to the use of pupil's full names. The school address, email and main telephone number should be the only contact information available to website visitors.

The uploading of any images or photographs of pupils onto the school website required parental consent. Any images should be carefully chosen with safeguarding in mind.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Complaints:

Complaints regarding pupil misuse of the school's internet, email etc … will be dealt with by SLT, DSL, pastoral managers and IT Support team.

Sanctions for misuse may include :

- Revocation of internet, school network use privileges
- Communication with pupil's parents, guardians and carers
- Detention or other usual discipline methods

Monitoring
The law related to internet use if changing rapidly and staff and pupils need to be aware of this. Relevant laws include :

- The Computer Misuse Act 1990
- The Public Order Act 1986
- The Communications Act 2003
- The Sexual Offences Act 2003
- The Malicious Communications Act 1988
- The Copyright, Design and Patents Act 1988
- The Protection of Children Act 1978
- The Obscene Publications Act 1959 and 1964
- The Protection from Harassment Act 1997

The school will be aware of and responsive to any issues experience via their use of the internet or digital technology outside of school. This policy should be monitored and updated to account for changes in the legal landscape, such as amendments to the above outlined laws and Acts.

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)
- DfE (2003) Filtering and Monitoring standards for Schools and Colleges
- DfE (2021) Harmful Online Challenges and Online Hoaxes
- DfE Keeping Children Safe in Education 2025
- DfE (2022) Teaching Online Safety in School
- DfE (2022) Searching, Screening and Confiscation
- Department for Digital, Culture, Media and Sport UK Council for Safer Internet (2020) Sharing Nudes and semi-nudes: advice for educational setting working with children and young people
- UK Council for Child Internet Safety (2020) Education for a Connected World – 2020 Edition

This policy operates in conjunction with the following school policies :

- Acceptable Use Policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Relationships and Sex Education (RSE) Policy
- Behaviour and Discipline Policy
- GDPR Data Protection Policy
- Mental Health and Emotional Wellbeing Policy

This policy will be monitored and updated to account for changes in the legal landscape, such as amendments to the outlined laws and Acts.

Use of devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Acceptable Use Agreement

Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the Principal conduct half-termly light-touch reviews of this policy to evaluate its effectiveness. The trustee board, Principal and DSL will review this policy in full on an annual basis and following any online safety incidents.

Any changes made to this policy are communicated to all members of the school community.

The next scheduled review date for this policy is **July 2026**.