Online Safety Policy

Prepared/Updated : April 2024

Review Frequency : Annually

Next Review Due : April 2025

Statement of intent

This policy is intended to ensure pupils at Penwortham Priory Academy are protected while using digital technologies at the Academy.

Penwortham Priory Academy is committed to including digital technologies, in particular internet use, in our curriculum. In doing so, we recognise the inherent risks posed by this useful learning tool. Full compliant with this policy will mitigate these risks and help to ensure pupils are safe online.

Introduction

New technologies have become integral in the lives of children and young people in today's society, both within schools and their lives outside school.

While digital technology and the internet provide an exciting opportunityfor pupils to learn and interact with various subjects, they also pose a risk, with the potential for exposure to inappropriate content and inappropriate contact from other children and adults. Digital technology also provides an opportunity for pupils to engage in unacceptable behaviour, both online and offline.

In order to keep pupils safe online, and for them to learn how to keep themselves safe online, all pupils and teachers should be aware of relevant skills and strategies needed to ensure internet safety. This ranges from knowing to only use the internet with adult supervision foryounger pupils, to strategies for identifying appropriate links for older children.

Mitigating the risk to pupils created by digital technology and the internet will be ensured through specific online safety lessons and will also be embedded within the general curriculum.

Online safety will depend on policies being properly implemented at alllevels of the school community: from published policies, to a secure school network design, the effective management of school broadbandand filtering systems, parental awareness of the dangers of online useand effective teaching about digital-technology use.

The Department for Education (DfE) categorizes the dangers above into four areas of risk (knowns as 4Cs) :

- **Content** : being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalization and extremism.
- **Contact** : being subjected to harmful online interaction with other users; for example : child on child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **Conduct** : personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images (eg. consensual and non-consensual sharing of nudes and semi-nudes and / or pornography, sharing other explicit images and online bullying; and
- **Commerce** : risks such as online gambling, inappropriate advertising, phishing and or financial scams

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. Keeping Children Safe in Education 2024.

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.

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 / ClassCloud 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 appropriate shared 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.

Responsibilities

Trustees

Trustees are responsible for approving the Online Safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Trustees receiving regular information about online incidents and monitoring as part of the Principals termly report.

The nominated safeguarding Trustee, Dr Phil Range has taken on the role of Online Safety Trustee. The role of Online Safety Trustee is

- Liaise with Online Safety designated person
- Reporting to relevant Trustees committee / meetings

Principal and SLT

- Principal is responsible for ensure the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the online designated person
- The leadership team are responsible for ensuring that the Online Safety person and other relevant staff receive suitable CPD to ensure them to carry out their online safety roles and to train other colleagues, as relevant.
- A member of SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Online Safety Designated Person

- Takes day to day responsibility for online safety issues
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place, including recording of incidents on CPOMs
- Organises training for staff
- Liaises with local authority
- Liaises with ICT staff and Lead of Computing
- Receives reports of online safety incidents and creates a log to inform future online safety developments

- Liaises with Online Safety Trustee to discuss current issues
- Attends relevant meeting / committee with Trustees
- Reports regularly to SLT

Network Manager / ICT Staff

Responsible for ensuring that :

- they meet regularly with Principal to discuss ICT infrastructure and that it is secure and is not open to misuse or malicious attack
- liaising with SLT and Online Safety Designated person with regards to any IT updates related to monitoring the school network / system
- the school meets the online safety technical requirements and any relevant Local Authority Online Safety guidance
- The school's filtering procedure is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- They keep up to date with e-safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- The use of the network / Virtual Learning Environments (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Designated person for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school procedures

Teaching Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the Online Safety Designated person / Network Manager / ICT team for investigation / action / sanction via Technical Services / record on Synergy / CPOMS if appropriate.
- Digital communications with pupils (emails, TEAMs etc …) should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school online safety and acceptable use policy

- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated person for Child Protection

Should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Online bullying
- Online materials related to extremism and radicalization

Pupils

- are responsible for using the school ICT systems in accordance with the acceptable use policy, which they will be expected to agree to before given access to the school system
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and other hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realize that the school's online safety policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / carers play a crucial role in ensuring that their child / children understand the need to use the internet / mobile devices in an appropriate way. Parents / carers will be responsible for accessing the school website / Synergy in accordance with the relevant school usage.

Education – how pupils are taught to keep themselves safe

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in Online Safety is therefore an essential part of the school's Online Safety provision.

Children need the help and support of the school to recognize and avoid Online Safety risks and build their resilience, whilst using social media and games consoles in particular.

Online Safety education will be provided in the following ways :

- A planned Online Safety programme as part of PSHE / LfL curriculum
- Key Online Safety messages should be reinforced by the Online Safety SLT lead, as part of a planned programme of assemblies, tutorial and pastoral activities.
- Pupils should be taught in their lessons to be critically aware of the material / content they access online and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the acceptable use policy and encouraged to adopt a safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils should be taught to acknowledge the sources of information used to and respect copyright when using material accessed on the internet.
- Pupils should also be reminded how to report any online safety incidents through school

Online Safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet eg. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Through PSHE, LfL and other lessons, by the end of secondary school, pupils will know :-

- Their rights, responsibilities and opportunities online, including the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has

the potential to be shared online and the difficulty of removing compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (eg. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (those created by children) is a criminal offence which carries penalties.
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours inline (eg. bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognize consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

Where necessary, teaching about safeguarding, including online safety will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Education - Parents / Carers
Some parents / carers may have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online experiences.

Parents / carers often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide" (Tanya Byron report). The school will therefore seek to provide information and awareness to parents / carers through :

- Parents newsletters including Safeguarding
- Parents evenings
- Website – Online Safety
- Information about local / national online safety campaigns / literature
- School events

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 2024
- 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

Training – 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 organisation.

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 (eg. 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/onlinewithout 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. Identify theft (including hacking Facebook profiles).

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 Team at 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. • Machines 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.

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.

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.

Schedule for Monitoring / Review

This online safety policy was approved by SLT	April 2024 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 2024, in readiness for the new term, September 2024
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 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 BfL policy then :

Low Severity

For example :

- misuse of school email
- off task on the internet

Member of staff follows procedures from Priory's Behaviour policy

Logs incident on Synergy

Medium Severity

For example :

- inappropriate sites
- bypass filters
- playing games

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

Incident directly reported to Online Designated Lead / DSL / Pastoral managers – follow procedures from Priory's Behaviour 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 Synergy 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 Designated Lead, DSL, Pastoral managers who will discuss with Principal.

Online Designated Lead receives alert through ClassCloud / LightSpeed – follow procedures from Priory's Behaviour 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 Synergy and on CPOMs

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

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 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 2023
- 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 Well-Being 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.