Pendle
Education Trust

COLNE PRIMET ACADEMY

Online Safety Policy

Author of Policy	Carl Thomas, DSL
Policy Approved by	Local Academy Council
Date	October 2026
Review Date	October 2027

Pendle Education Trust
Nelson and Colne College, Scotland Road, Nelson, BB9 7YT
Tel 01282 440 249 Email contact@pendleeducationtrust.co.uk
Company Registration Number: 08263591
Place of Registration: England and Wales

Contents

1. Aims 3
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating pupils about online safety 6
5. Educating parents/carers about online safety 8
6. Cyber-bullying 8
7. Acceptable use of the internet in school 10
8. Pupils using mobile devices in school 16
9. Staff using work devices outside school 16
10. How the school will respond to issues of misuse 17
11. Training for staff, governors and volunteers 22
12. Monitoring arrangements 23
13. Links with other policies 23
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers) 24
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) 26
Appendix 4: online safety training needs – self-audit for staff 28
Appendix 5: online safety incident report log 29

1 1. Aims

Colne Primet Academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news), and conspiracy theories
- **Contact** – being subjected to harmful online interaction with other users or generative AI applications that simulate this, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct** – online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), including those generated using AI, and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2 2. Legislation and guidance

This policy is based on the statutory safeguarding guidance, Keeping Children Safe in Education from the Department for Education (DfE) and its advice for schools on:

- Teaching online safety
- Meeting digital and technology standards
- Preventing and tackling bullying
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation
- Mobile phones in schools

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Children's Wellbeing and Schools Act 2026 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3 3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will ensure online safety is a running and interrelated theme in the whole-school approach to safeguarding and related policies and procedures, including when planning the curriculum, teacher training, the role of the DSL (and deputies) and any parental engagement.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and that a review of the effectiveness of the filtering and monitoring systems is carried out by SLT at least once every academic year. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

All governors will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

They will make sure that there are robust cover arrangements for when the DSL is unavailable due to illness, leave or other circumstances – for example, a confidential shared mailbox to make sure safeguarding concerns are received, monitored and acted on without delay.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by informing the DSL, including Deputy DSLs, and the IT support department.
- Following the correct procedures by e-mailing the DSL, including Deputy DSLs, and the IT support department if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4 4. Educating pupils about online safety

4.1 Pupils will be taught about online safety as part of the curriculum

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **KS3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and/or may post things which aren't real/have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images
- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- How information and data is generated, collected, shared and used online
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion

- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

The safe use of social media and the internet will also be covered in other subjects where relevant.

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

4.2 Pupils will be taught practical cyber security skills

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The physical security of devices
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyber-bullying and the risks of online radicalisation.

5 5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or weekly e-bulletins. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online
- The school's expectations in respect of appropriate use of AI by pupils

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6 6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form Tutors will discuss cyber-bullying with their Tutor Groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device in line with the school's searching and confiscation policy ADD SEARCH POLICY

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL/headteacher/other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed

to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), including any image generated or altered by AI, they will not:

- View, copy, print, share, store, save, forward on, or ask a child to share or download, the image
- Delete the image or ask the pupil to delete the image
- Ask the pupil(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL
- Share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers
- Say or do anything to blame or shame any pupil involved

The staff member will confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

If the staff member has already viewed the imagery by accident (e.g. if the pupil showed it to them before they could ask them not to), they will report the incident to the DSL and seek support.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy/searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Colne Primet Academy recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes' or 'deep nudes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Colne Primet Academy will treat any use of AI to bully pupils very seriously, in line with our Prevention of bullying policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by Colne Primet Academy and Pendle Education Trust, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence is carried out in line with our AI usage policy.

7 7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences – harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering *Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					**X**

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990):	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent children becoming involved in cyber-crime and harness their activity in positive ways – further information here.					**X**

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright and intellectual property (including through the use of AI services)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

When undertaken for non-educational purposes and using school devices / systems (unless otherwise stated)	Staff and other adults				Children	
	Not allowed	Allowed	Allowed at certain times/places	Allowed for selected staff	Not allowed	Allowed
Online gaming			X		X	
Online shopping / commerce			X		X	
File sharing			X		X	
Social media (personal use)			X		X	
Social media (professional use – PET /PPA accounts)		X			X	
Messaging / chat			X		X	
Entertainment streaming services (when used legally)			X		X	
Use of video broadcasting, e.g. YouTube, TikTok			X		X	
Personal mobile phones brought in to school		X				X**
Use of personal mobile phones in school			X*		X	
Taking photos / images on personal mobile phones			X		X	
Use of other perianal digital devices, including tablets, gaming devices and smart watches	X				X	
Use of personal email accounts on school devices and/or school network/WiFi	X					X***
Use of school email for personal communication	X					X****

When undertaken for non-educational purposes and using school devices / systems (unless otherwise stated)	Staff and other adults				Children	
	Not allowed	Allowed	Allowed at certain times/places	Allowed for selected staff	Not allowed	Allowed
Use of AI services that have not been approved by school.	X				X	

*Photos should only be taken on personal devices, when a school device is not available. Photos taken on personal devices should only be taken for the purpose of uploading to social media accounts or transferring onto school systems and then must be instantly deleted from the personal device, including any cloud or online linked storage/backup.

**In appropriate circumstances, students may use personal email accounts for the purpose of accessing online work stored on personal accounts, in order to aid in the completion of coursework and/or non-exam assessments.

***In appropriate circumstances, students may use their school e-mail account to communicate with professional bodies, under the guidance of their teachers or Primet Academy staff. For example, when applying for work experience placements and/or college applications.

8 8. Pupils using mobile devices in school

In line with statutory guidance, our school is a mobile phone-free environment by default. Pupils are not permitted to have access to or use their mobile phones or smart technology with similar functionality to mobile phones (e.g. smart watches), which we refer to collectively as 'mobile phones', throughout the school day. This prohibition includes all lessons, the time between lessons, breaktimes, and lunchtimes.

Any deviation from this mobile phone-free baseline will be by exception only (for example, approved arrangements for specific medical tracking or documented safeguarding needs) and must be explicitly authorised by the headteacher.

Where there is an arrangement by exception, any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2). Any breach of the acceptable use agreement by a pupil may trigger a sanction in line with the school behaviour policy, which may result in the confiscation of their device.

****Students are allowed to bring mobile phones into school to support with transport, travel arrangements and safety before and after school so that they are able to communicate with family and friends. Students must follow the Acceptable Behaviour Policy in relation to use of mobile phone on school site, which are banned.

9 9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.
Work devices must be used solely for work activities.
If staff have any concerns over the security of their device, they must seek advice from the academies IT Support department and the IT Manager.

10 10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received.
- The DSL and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures, this may include:

        - Non-consensual images
        - Self-generated images
        - Terrorism /extremism
        - Hate crime/ Abuse
        - Fraud and extortion
        - Harassment/stalking
        - Child Sexual Abuse Material (CSAM)
        - Child Sexual Exploitation Grooming
        - Extreme Pornography
        - Sale of illegal materials/substances
        - Cyber or hacking offences under the Computer Misuse Act
        - Copyright theft or piracy
- Any concern about staff misuse will be reported to the Principal, unless the concern involves the Principal, in which case the complaint is referred to the Director for Education.
- Where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss.

Where there is no suspected illegal activity, devices may be checked using the following procedures:

- One or more members of SLT should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated device that will not be used by children and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
- Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed and signed by the members of SLT conducting the check.
- Once this has been completed and fully investigated the members of SLT will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by Pendle Education Trust
    - Police involvement and/or action
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.

- There are support strategies in place e.g., peer and/or wellbeing support for those reporting or affected by an online safety incident.
- Incidents should be logged. Incidents involving children will be logged, including actions taken on CPOMS. Incident involving adults, including actions taken on StaffSafe.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.
- Learning from the incident (or pattern of incidents) will be provided anonymously and redacted as required to:
    - The DSL Cluster and Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with.
    - Staff, through Safeguarding Briefs and/or staff meetings
    - Children through assemblies and lessons
    - Parents/carers, through newsletters, school social media, website
    - Local academy council and PET Board through regular safeguarding updates and reporting.
    - Local authority/external agencies, as relevant

The school will make the flowchart on the following page available to staff to support the decision-making process for dealing with online safety incidents.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

The Prevent duty, outlined in the Counter-Terrorism and Security Act 2015, requires schools to have "due regard to the need to prevent people from being drawn into terrorism." This includes addressing the risk of online radicalisation. Colne Primet Academy recognises that the internet and social media can be used to spread extremist ideologies.
The school has robust filtering systems to block access to extremist content, working alongside robust monitoring procedures to identify potentially concerning online activity.

Online safety education is integrated across the curriculum, including lessons at an age and developmentally appropriate level on:

- Identifying and reporting extremist content.
- Understanding the dangers of online grooming and manipulation.

- Promoting British values.

Safeguarding procedures are in place to address concerns about potential radicalisation. This includes clear reporting mechanisms and collaboration with relevant agencies. *See also: Prevent Duty Risk Assessment and Procedure.*

The school communicate with parents about online safety and the Prevent duty through the school newsletter, website and online safety information events, including at parent evenings. The school provides resources and guidance to help parents/carers keep their children safe online.

Responding to incidents involving children's actions

Incidents	Refer to class teacher	Refer to Head of Year	Refer to DSL or Principal	Refer to Police / CSC	Refer to PET IT Team for support / action	Inform parents/carers	Remove device / internet access rights	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).			X	X	X	X	X	X
Attempting to access or accessing the school network, using another user's account (staff or child) or allowing others to access school network by sharing username and passwords		X			X	X		X
Corrupting or destroying the data of other users.		X			X	X	X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X				X	X	X
Unauthorised downloading or uploading of files or use of file sharing.		X			X	X	X	X
Using proxy sites or other means to subvert the school's filtering system.		X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.			X		X	X		
Deliberately accessing or trying to access offensive or pornographic material.			X		X	X	X	X

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X				X		X
Unauthorised use of digital devices (including taking images)		X	X			X	X	X
Unauthorised use of online services		X				X		X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X	X			X	X	X
Continued infringements of the above, following previous warnings or sanctions.			X			X	X	X

Responding to incidents involving staff actions

Incidents	Refer to line manager	Refer to Principal	Refer to Police and/or LADO	Refer to IT and Network Support Team for action	Further action, in line with disciplinary procedures
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X	X
Actions which breach data protection or network / cyber-security rules.		X		X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		X	X
Using proxy sites or other means to subvert the school's filtering system.		X		X	X
Unauthorised downloading or uploading of files or file sharing		X		X	X
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems)		X		X	X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.		X		X	X

Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X	X
Using personal e-mail/social networking/messaging to carry out digital communications with children and parents/carers		X		X	X
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X	X		X	X
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X	X			
Actions which could compromise the staff member's professional standing	X				
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X		X	X
Failing to report incidents whether caused by deliberate or accidental actions	X	X		X	
Continued infringements of the above, following previous warnings or sanctions.		X			X

11 11. Training for staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, including images generated or altered by AI, especially around chat groups
- Sharing of abusive images and pornography, including images generated or altered by AI, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and Deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

12 12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.
This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13 13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Mobile phones policy
- AI policy

Appendix 1: KS3 and KS4 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others
- Only use generative AI in accordance with the school's [AI policy]
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate, including anything created using AI
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will make sure it's switched off and [stored away securely/handed in – delete as appropriate] as required by school rules immediately upon entering the school
- I understand that I am not permitted to look at, use, or have access to my device at any point during the school day – including during lessons, the time between lessons, breaktimes, and lunchtimes
- I will only use my device if I have official written permission from the school
- I agree that if I break the school rules on mobile devices, my device will be confiscated

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and regarding a default ban on mobile devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

14 Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS
Name of staff member/governor/volunteer/visitor:
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: › Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) › Use them in any way that could harm the school's reputation › Access social networking sites or chat rooms › Use any improper language when communicating online, including in emails or other messaging services › Install any unauthorised software, or connect unauthorised hardware or devices to the school's network › Input, upload, or process any personal data of pupils, confidential safeguarding information, or sensitive school data into public or unvetted generative AI tools (such as public AI chatbots or image generators). I will make sure I am aware of approved AI tools for use in school and follow this at all times › Share my password with others or log in to the school's network using someone else's details › Take photographs of pupils without checking with teachers first › Share confidential information about the school, its pupils or staff, or other members of the community › Access, modify or share data I'm not authorised to access, modify or share › Promote private businesses, unless that business is directly related to the school
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too. I will use generative AI in line with the school's [AI policy].

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Signed (staff member/governor/volunteer/visitor):	**Date:**

15 Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

16 Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**