Pinewood Infant School & Foundation Unit

Online Safety Policy

Autumn 2025

Development/Review/Monitoring

This Online Safety Policy has been developed by:

- Rachel Otter, Head Teacher/Online Safety Lead
- Kellie Reilly, Assistant Online Safety Lead
- Staff – including Teachers, Support Staff, Technical staff
- Governors

Consultation with the whole school has taken place through a range of formal and informal meetings.

Schedule for development/Review/Monitoring

This Online Safety Policy was approved by the Governing Body in:	Autumn term 2025
The implementation of this Online Safety Policy will be monitored by the:	*Online Safety Lead/Head Teacher/Safeguarding Lead – Ms Rachel Otter* *Assistant Online Safety Lead – Miss Kellie Reilly*
Monitoring will take place:	*By Head Teacher and Assistant Online Safety Lead once a year or after any KCSIE reviews*
The governing body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents)	*Once a year and termly record of any breaches*
The Online Safety Policy will be reviewed annually, or more regularly if there are any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Autumn 2026*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys/questionnaires of pupils, parents/carers and staff

Scope of the policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of school digital technology systems, both in and out of school. The Education and Inspections Act 2006 empowers head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying or other online safety incidents covered by this policy, which may take place outside of school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for, and of, electronic devices and the deletion of data. In the case of both Acts, action can only be taken over issues covered by the published Behaviour Policy.

Pinewood Infant school will deal with such incidents within this policy and associated Behaviour and Anti-Bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Links to other policies

This policy links with the following policies and forms part of our Safeguarding procedures here at Pinewood Infant School and Foundation Unit:

- KCSIE 2025
- Child Protection Policy
- Acceptable Use Agreement
- Computing Policy
- Behaviour Policy
- Remote Learning Policy
- Device Loan Agreement
- Social Media Policy
- Cyber Protection Policy

At Pinewood, we understand that keeping children safe online is a vital part of our safeguarding responsibilities. As outlined in Keeping Children Safe in Education (KCSIE) 2025, technology is part of everyday life, even for our youngest learners, and brings both opportunities and risks.

We are committed to:

- Embedding online safety throughout our safeguarding policies and daily practice.
- Using effective filtering and monitoring systems on all school devices and networks, and regularly reviewing their effectiveness.
- Ensuring that all staff receive ongoing training so they understand online risks, the systems we use, and how to respond to concerns.
- Providing age-appropriate teaching so that children begin to understand how to stay safe online, ask for help, and build resilience.
- Engaging with parents and carers to share advice and resources that help families keep children safe at home as well as in school.
- Reviewing our practice regularly to respond to new and emerging online risks.
- Protecting children from the four key categories of online risk: Content, Contact, Conduct, and Commerce – now including the risks of misinformation, disinformation and conspiracy theories.

The Content category now explicitly includes misinformation, disinformation (including fake news), and conspiracy theories. Our curriculum and safeguarding approach will therefore support children to develop critical thinking, media literacy, and digital resilience to help them question and assess information they encounter online. Pinewood furthermore considers its procedures for using AI. With considerations for of both a pupil and staff approach. With recognition for both administrative and curriculum tasks.

The Designated Safeguarding Lead (DSL) – Ms Rachel Otter has overall responsibility for online safety within our safeguarding framework, but keeping children safe online is the responsibility of every adult in our school community

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals within the school.

Governing Body

The governing body are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by governors receiving regular information about online safety incidents and monitoring reports. The Online Safety Governor is Rachel Makey and the role will include:

- Monitoring of online safety incident logs.
- Reporting to relevant governors/committee/meetings.

Head Teacher

- The head teacher (who is also the school's DSL) has a duty of care for ensuring the safety (including online safety) of members of the school community, although the day to day responsibility for online safety will be delegated to the Assistant Online Safety Lead, Kellie Reilly.
- The head teacher and deputy head teacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The head teacher and deputy head teacher are responsible for ensuring that the Assistant Online Safety Lead, Kellie Reilly and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Online Safety Lead and Assistant Online Safety Lead will meet regularly to monitor online safety practices as a school.

Online Safety Lead/Assistant Online Safety Lead

The Online Safety Lead and Assistant Online Safety Lead:

- Take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school Online Safety policies/documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provide training and advice for staff
- Liaise with the Local Authority when necessary
- Liaise with school technical staff
- Receive reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Meet with Rachel Makey - Online Safety Governor to discuss current issues, review incident logs and filtering
- Report regularly to the governing body

Network Manager/Technical Staff

We have a managed ICT service provided by Jeff Lee, ICT Services. He works with the technical staff and they are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements
- That users may only access the networks and devices through a properly enforced password protection procedure, in which passwords are regularly changed (90 days)
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network/internet/learning platforms/remote access/email is regularly monitored in order that any misuse or attempted misuse can be reported to Rachel Otter or Kellie Reilly for investigation/logging/action/sanction
- That monitoring software/systems are implemented and updated as agreed
- That monitoring software/systems are reviewed on a termly basis with SLT and IT provider. Findings are then presented to the governing body

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 procedures
- They have read, understood and signed the Staff Acceptable Use policy/Agreement
- They report any suspected misuse or problem to Rachel Otter or Kellie Reilly for investigation, action and/or sanction
- All digital communications with pupils/parents/carers 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 activities
- Pupils understand and follow the Online Safety policy and Acceptable Use Agreement/policy
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be only 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 and any issues are reported to the Online Safety Lead.
- That they receive online safety training yearly

Designated Safeguarding Lead

Designated Safeguarding Leads, Rachel Otter and Dave Armstrong-Jones should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Online bullying

It is important to remember that these are safeguarding issues, not technical issues, because the technology provides additional means for safeguarding issues to develop.

They will ensure that they:

- Understand how filtering/monitoring systems work.
- Receive and review reports on their effectiveness at least annually.
- Ensure that staff and pupils are trained in the latest online risks, including misinformation, disinformation, and AI.

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety policy covers their actions out of school, if related to their membership of the school
- Will be taught the **SMART** rules and follow them when using digital devices in school

Education - Pupils

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/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/PSHE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of planned assemblies
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. *N.b. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet (at an age appropriate level)*
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that 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
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- All online safety education must be age appropriate and tailored to meet the needs of all individuals

Online safety education will now include media literacy skills, teaching children how to:

- Recognise false or misleading content
- Question online sources and bias
- Build resilience to manipulation online

These skills will be embedded across Computing, PSHE, and RSHE lessons in an age-appropriate way.

Education - Parents/Carers

Many parents and carers 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 behaviours. Parents/carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website, Learning Platforms, Class DoJo, online safety leaflets
- Parents/Carers evenings
- High profile events/campaigns e.g. Safer Internet Day, workshops for parents
- Reference to the relevant websites/publications
- Online safety training offered to parents/carers yearly
- Specific app information shared with parents/carers

Education - The Wider Community

Pinewood Infant School will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in the use of new digital technologies, digital literacy and online safety when appropriate
- Online safety messages targeted towards grandparents and other relatives as well as parents/carers
- The school website will provide online safety information for the wider community

Education & Training

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:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements and these will be carried out yearly
- The assistant online safety lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations and feed back to online safety lead
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings/INSET days
- The online safety Lead/assistant lead will provide advice/guidance/training to individuals as required

Training - Governors

Governors take part in online safety awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety/safeguarding.

This may be offered in a number of ways:

- Attendance at external training or training online
- Participation in school training/information sessions for staff or parents/carers

Technical - Infrastructure/Equipment, Filtering and Monitoring

Pinewood Infant school is responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

Pinewood Infant School technical systems will be managed in ways that ensure that the school meets recommended technical requirements by the following:

- Systems will be reviewed and tested at least annually to ensure they are effective, age-appropriate, and proportionate and they will be benchmarked against the DfE's "Plan Technology for Your School" service to ensure compliance with national standards.
- Pinewood will be able to respond to emerging risks, including AI-generated content, dynamic online material, and evolving harmful behaviours.
- Servers, wireless systems and cabling that are securely located and their physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.

- The “master/administrator” passwords for the school ICT systems, used by Jeff Lee, Network Manager or Technical Staff, School Business Manager, Dave Armstrong-Jones, Kellie Reilly must also be available to the Head Teacher, Rachel Otter.
- The online safety lead is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Ensuring that internet access is filtered for all users. Illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored.
- Ensuring that internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Providing enhanced/differentiated user-level filtering.
- School technical staff, online safety lead and assistant lead monitor the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc, from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy through GDPR arrangements are is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Responsibility for overseeing filtering and monitoring lies with the Designated Safeguarding Lead (DSL), working with the IT lead and governors. The DSL must understand how the systems operate, review alerts, and ensure appropriate escalation of concerns.

Mobile Technologies (including Bring Your Own Device - BYOD)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school’s wireless network. The device then has access to the wider internet which may include the school’s learning platforms and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s online safety education programme.

- The school Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies

The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Pupil owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*

School owned/provided devices:

- Laptops are issued to every teacher which allows them to access the school's network
- Teacher laptops are allowed off the school premises but staff must follow the Security Handling Policy procedures when doing so
- Laptops are encrypted with passwords which are changed regularly
- All teaching and admin staff have network logins and have access to the resources and staffroom drives on the server
- Head Teacher, Deputy Head Teacher, ICT Lead and office logins have access to all drives, including the shared drive
- Jeff Lee, Kellie Reilly and Dave Armstrong-Jones have administrator logins
- All devices have filtering and monitoring certificates installed
- If a staff member leaves employment at the school then their logins and data will be removed

Personal devices:

- The use of personal mobile phones on site is allowed by staff in designated areas, agreed by the head teacher
- Visitors are allowed to bring their personal mobile phones onto the premises but use is only allowed in designated areas
- Personal mobile phones are kept out of sight of children when not in use
- Staff can use their own portable storage devices (memory stick, hard drive, etc) but all are encrypted by ICT lead
- Staff are not permitted to use personal laptops on site unless agreed by Head teacher/ICT Lead
- Staff can attach to our school Wifi but certain programmes will not be accessible due to our Smoothwall monitoring and filtering. A trust certificate will be installed by ICT Lead when necessary
- All new visitors into school will read and sign the visitors acceptable use agreement

Use of Digital and Video Images

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, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry 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 risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital / video images
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs

Personal Data

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school ensures that:

- It has a Data Protection Policy
- It has appointed a Data Protection Officer (DPO) – Dave Armstrong-Jones
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out**.**
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures are in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.

- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- We have a Freedom of Information Policy which sets out how it will deal with FOI requests
- All staff receive data handling awareness/data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising 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.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected following the school's mandatory password procedure.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies have the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

When using communication technologies the school considers the following as good practice:

- The official school email service (Office 365 – Outlook) is regarded as safe and secure and is monitored. Users are made aware that email communications are monitored.
- Any digital communication between staff and parents/carers (email, Class DoJo, text messages) must be professional in tone and content **(*Personal email addresses, text messaging or social media must not be used for these communications*).**
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or Local Authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published.
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or Local Authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established there should be:

- A process for approval by senior leaders.
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff.
- A code of behaviour for users of the accounts, including systems for reporting and dealing with abuse and misuse.
- Understanding of how incidents may be dealt with under school disciplinary procedures.

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is impacting duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites.

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the internet for public postings about the school.

The school should effectively respond to social media comments made by others according to a defined policy or process. (See social media policy).

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing inappropriate content or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyberbullying would be banned and could result in criminal prosecution. There are however a range of activities which may, generally be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. Pinewood Infant 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 or outside the school when using school equipment or systems. The school policy restricts usage as follows:

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, these will be reported to the police immediately.

Other Incidents

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

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the Police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should 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, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group 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 disciplinary procedures
    - Involvement by the local Authority
    - Police involvement and/or action

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:

- Incidents of 'grooming' behaviour
- The sending of obscene materials to a child
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Promotion of terrorism or extremism
- Other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation. It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Cyber Security

At Pinewood we recognise that effective cyber security is a vital part of safeguarding and of our duty to protect children, staff and school systems. As highlighted in Keeping Children Safe in Education (KCSIE) 2025, schools must take active steps to reduce risks from cyber-attacks and to secure sensitive data.

We are committed to:

Protecting Systems and Data

- We will implement secure firewalls, anti-virus software, and system protections to prevent unauthorised access to our networks.
- All devices and software will be kept up to date with the latest security patches.
- Sensitive information about children, staff, and families will be stored securely and only accessed by authorised users.

Access Control and Passwords

- Strong password policies will be enforced for staff, pupils (where appropriate), and governors.
- Access to systems will follow the principle of "least privilege" — ensuring users only have the access necessary for their role.
- Multi-factor authentication will be used where possible for critical systems.

Staff Awareness and Training

- Staff will receive training to recognise phishing attempts, suspicious links, and other cyber threats.
- All staff will be expected to follow safe practices, such as locking screens, securing devices, and reporting concerns immediately.

Incident Response

- Any suspected cyber-attack or breach will be treated as a safeguarding incident and reported to the DSL, Headteacher, and IT lead without delay.
- The school will follow its incident response plan, which includes containment, investigation, notification, and recovery procedures.
- Serious incidents may be escalated to external agencies such as the DfE, local authority, police, or the National Cyber Security Centre (NCSC).

Regular Review and Testing

- Cyber security measures will be reviewed at least annually, or sooner if prompted by an incident or new risk.
- The school will benchmark its practice against the DfE's Cyber Security Standards to ensure our systems remain robust and proportionate

Artificial Intelligence – AI

The school acknowledges the growing role of artificial intelligence (AI) and other emerging technologies.

- Any AI or generative tools used by staff or pupils must be approved by the Online Lead and subject to safeguarding risk assessment.
- The school will ensure that filtering and monitoring systems are able to detect and manage AI-generated or manipulated content that may be harmful.
- AI use will always be supervised, transparent, and age-appropriate, with safeguarding considerations at the forefront.
- SLT and Assistant Online Safety Lead will undergo AI training annually.
- School refers to the Generative AI product safety expectations published by the DFE
- IF/when school chooses to use pupil facing AI, we must take great care to ensure we are abiding by our legal responsibilities including those related to
  - Data protection
  - KCSIE
  - Intellectual property law

- We will also consider possible impacts on learning, the importance of the teacher-pupil relationship and the risks of bias and misinformation.
- Staff must use their professional judgement when using these tools. Content produced requires critical assessment to check for appropriateness and accuracy.
- Online Safety Lead and IT manger will ensure that AI is turned off on iPads (the Siri function is disabled across all iPads)
- Staff are aware that Google may provide AI-generated responses, which may contain inaccuracies or misinformation, and they should therefore verify information from reliable and trusted sources before use.

School Actions and Sanctions

It is more likely that as a school we 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.

This policy, along with the effectiveness of filtering and monitoring systems, will be reviewed annually (Autumn term 2026 by the full Governing Body), or sooner if there are significant safeguarding incidents, technological developments, or updated DfE guidance.