Digital Technology at Pear Tree School

Last Reviewed: 11th June 2026

Individuals responsible for digital safety within school:

Headteacher/Responsible Individual: David Bartlett
Designated Safeguarding Lead (DSL): Gary Ramsbottom
SLT: Philip Tebbs and Helen Berry and Fiona Corner
IT Support: Mastercopy, Qustodio and Rachel Smith, Teacher

Related policies:
Safeguarding & Child Protection Policy
Behaviour Policy
Data Protection Policy
Staff Code of Conduct
Acceptable Use Policy
Whistleblowing Policy

Introduction

As stated by UK Council for Internet Safety (2020), students are growing up in a complex world both online and offline. It is crucial that we support them to enjoy childhood and allow them to benefit safely from all the opportunities online can bring to them. However, it is also important they learn to balance these benefits and stay safe, allowing them to make positive contributions to the online world. At Pear Tree School, we are committed to equipping our students with the skills and knowledge needed to flourish and succeed in an ever-changing digital society whilst maintaining the highest levels of safety and security, so our students are given the opportunity to recover and thrive after the adverse childhood experiences they have faced.

This policy supports compliance with the Education (Independent School Standards) Regulations 2014, particularly Part 3 (Welfare, Health and Safety of Pupils), Part 6 (Provision of Information) and Part 8 (Quality of Leadership and Management).

Aim

Our policy aims to outline how, as a school, we:

- Provide learning opportunities and promote digital safety across the school.
- Have measures in place in line with statutory requirements in order to safeguard students and staff.
- Recognise the ever-changing digital world and how we can support our students to use this effectively, including AI.
- Support our residential homes to provide the same level of guidance and work alongside them with the goal of supporting our young people.
- Are influenced by other policies within the company including but not limited to movies, video games, pornographic material and mobile phone use.

Digital Technology at Pear Tree School

Digital technology is used across the school in many ways. Students are given opportunities to use laptops and iPads as learning tools, to research information, as intervention and support tools, and to be presented learning opportunities in different ways. Depending on individual needs, students may use apps, websites, windows and other software, and can be presented work through images, videos, links and publications. All devices are school controlled and issued within the lesson. Teachers supervise all devices used and maintain a logbook to ensure they are aware of which devices are being used by which students.

Teachers use a range of digital tools to provide different learning opportunities and can access a range of different websites and resources including doodle learning, Kahoot and BKSB.

Within school, students are not allowed to use USB drives unless provided by a teacher. Any work that needs to be shared can be done using email and google drive.

In line with the company movies and video games policies, we follow the guidelines of age-related ratings and PEGI as well as determining the appropriateness of all media used for our specific students depending on their needs and risk assessments.

Digital Technology and The Curriculum

Our curriculum recognises that anyone can be vulnerable online and that this can fluctuate; however, our students may all be vulnerable due to past experiences and influences, lack of support and understanding. It is always important that we consider how we tailor learning to make sure everyone receives the education they need and deserve without causing further trauma or harm.

All students participate in online safety lessons and are reminded of the child friendly technology agreement they agree to at the beginning of each school year (Appendix A).

Within our curriculum, our learning objectives include:

- Basic use of laptops and iPads including how to access the internet.
- How to use search engines appropriately
- Generating safe passwords
- E-safety terminology
- Laws around online safety
- Online relationships
- Digital resilience
- Social media safety

All learning materials used are dependent on our students' individual needs and are resourced from trustworthy sources including but not limited to: NSPCC; UK Safer Internet Centre, SWGfL and Safewise.

Online Safety

Online safety is a vital element of digital learning. Students need to develop the knowledge and skills required to keep themselves and others safe when using online platforms. Online safety is a priority across the school. Students are taught about key issues such as protecting personal information, cyberbullying, and the safe and responsible use of social media.

Teachers regularly discuss and reinforce online safety during all digital learning opportunities and promote internet safety through class-based workshops and other learning activities. Online and cyber safety, along with digital resilience, are further strengthened through whole-school participation in Safer Internet Day.

Strong working relationships with residential houses ensure consistency for our students, with shared expectations around safety and levels of support. Due to the backgrounds and individual needs of some students, online safety measures may include high-level one-to-one supervision or restricted internet access when risks are assessed as too high.

Any online safety concerns are recorded and shared with the senior leadership team, house managers, and other professionals as required through lesson-by-lesson curriculum forms and inappropriate use of technology forms on our connect system.

Filtering and Monitoring at Pear Tree School

This applies to all employees of Pear Tree and aims to ensure that effective safeguarding when children are using the internet is at the heart of all decision-making. We have developed our policies and procedures and delivered guidance and training to ensure that we are prepared to safeguard our children while they are using the IT equipment we provide in our School. To provide this guidance, we have consulted DfE standards for filtering and monitoring and ensured compliance with Keeping Children Safe in Education (KCSIE, 2025).

This section includes the expectations and responsibilities for our school around effective filtering and monitoring.
When considering filtering and monitoring, filtering is used to provide a proactive and preventative measure that prevents staff and students from accessing inappropriate material by identifying and blocking content. Monitoring is a reactive measure and therefore does not block staff and students from accessing material but can observe inappropriate activity, allowing us to record this and act.

KCSIE (2025) refers to the 4 Cs that must be considered and appropriately planned for when filtering and monitoring student and staff activities online:

a. **content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories. RSHE guidance for 2026, published in summer 2025, introduces new content concerns, including:
    i) Online scams – for example, 'sextortion', where individuals are blackmailed using sexually explicit material.
    ii) AI-related risks, including the malicious use of deep fakes and chatbots.
    iii) Fake or AI-generated social media profiles.

    Pear Tree will include these in its PSHEE provision to help students learn how to recognise this kind of deception and sharpen their digital literacy.
b. **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
c. **conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
d. **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

As stated in DfE Filtering & Monitoring Standards, we have ensured that we have:

- Identified and assigned roles and responsibilities to manage filtering and monitoring systems.
- Ensured the review of our filtering and monitoring provision annually.
- Blocked harmful and inappropriate content without unreasonably impacting teaching and learning.

Developed effective monitoring strategies to meet the safeguarding needs of students and staff.

Roles and responsibilities within Filtering and Monitoring

The roles and responsibilities of managing filtering and monitoring systems are clearly identified to allow everyone to work together to safeguard students and staff effectively. Furthermore, the clarity ensures professional expertise is used to make informed decisions. As head teacher, David Bartlett holds overall responsibility for filtering and monitoring and assuring the standards are met.

DSL- Gary Ramsbottom and Deputy DSL's- Philip Tebbs, Helen Berry and Fiona Corner (all part of the Senior Leadership Team).

As detailed in KCSIE (2025), our DSL leads on safeguarding and online safety. Specific duties include:

- checking relevant reports
- responding to safeguarding concerns identified by filtering and monitoring
- assuring that filtering and monitoring systems are working effectively and reviewed regularly

The SLT are responsible for:

- buying filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of our provision
- overseeing reports

They are also responsible for making sure that all staff understand their role and are appropriately trained to follow policies, processes and procedures and act on reports and concerns.

In-House IT Support- Rachel Smith, Teacher

Responsibilities include:

- Support to purchase systems and identifying risks.
- Supporting reviews.
- Carrying out checks including identifying school devices and ensuring software is applied.
- Ensure all staff are up to date with online safeguarding procedures and training (alongside training manager).
- Provide half termly monitoring information and data including any incidents.
- Ensure internet filtering and monitoring logs are up to date and provide new ones if necessary.
- Ensure users are identifiable to the school, so concerns can be traced back to individuals (Laptops are all assigned a number to be identifiable)

Third-Party IT Support provided by Mastercopy and Qustodio (Filtering system)

Responsibilities include:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or system checks

Review of filtering and monitoring annually

As part of the annual safeguarding review, the DSL, with the support from IT support and SLT, completes a Filtering and Monitoring review to ensure the needs of the children and staff are being appropriately met. This information can be requested and made available to anyone who is entitled to inspect it.

The annual review is carried out in line with the DfE Meeting Digital and Technology Standards in School and Colleges document. This annual review of our approach considers and reflects the risks that our students face, both collectively as technology and apps change, and individually in terms of their own circumstances.

A review will take place, as a minimum annually, or if:

- a safeguarding risk is identified
- There is a change in working practice, like remote access or BYOD
- new technology is introduced, such as new devices
- major software updates occur
- there are changes to the technical configuration of the network and devices

Blocking harmful and inappropriate content without unreasonably impacting teaching and learning:

The filtering software currently used, Qustodio, blocks access to harmful sites and alerts two of the SLT via email to ensure any action required is effectively managed. DSLs and SLT are responsible for ensuring that there is an appropriate response to the alert. This may include assigning it to a particular staff member to review and investigate and taking necessary steps in accordance with the Safeguarding Policy.

Currently, the software does not identify individual use. To identify individual use, each school-managed device has an assigned number. It is the responsibility of the teacher to log in to an internet filtering and monitoring device log which student is using which device to ensure all students can be supported correctly for inappropriate or illegal material.

In June 2026 Pear Tree School have installed Smoothwall onto all school managed devices to improve the filtering and monitoring system and to streamline reporting and information gathering for the DSL and SLT. This software update will also provide different levels of filtering and monitoring for individuals including students and staff.

Effective monitoring for safeguarding students and staff

Whilst all school-managed devices are used both on and offline, students are monitored in-person. Classrooms have a maximum of 5 students in order to manage this effectively. Furthermore, members of staff including Teaching Assistants and Residential Social Care Workers are utilised to support supervision levels when necessary. If required, students may be physically moved to enable all laptop screens to be monitored at the same time. The Designated Safeguarding Lead (DSL) is responsible for any safeguarding and child protection matters that are identified through monitoring.

Generative Artificial Intelligence (AI)

When discussing Generative Artificial Intelligence, it refers to technology that can be used to create new content based on large volumes of data that models have been trained on a variety of sources (DofE 2025).

As stated by the DofE (2025), Generative AI presents exciting opportunities to improve people's lives. If used safely, effectively and with the right infrastructure in place, AI can support every child and young person, regardless of their background, to achieve at school and college and develop the knowledge and skills they need for life. As a school, we support teachers to use AI to support them to do what they do best and encourage its use to reduce administrative burdens that staff face on a day-to-day basis.

The evidence of Generative AI and its benefits and risks to students using it is still emerging and we must ensure that we remain informed by research and case studies. It is important whilst teaching students that the risks alongside the opportunities and benefits as well as each student's experiences and understanding are all considered and inform our judgement.

At the time of writing this policy, all students are taught what AI is and the risks and benefits to individuals and society; however, it is not used by students. This will continue until we can ensure we can safeguard our students effectively in accordance with the current guidance.

DfE guidance on Generative AI (August 2025) identifies product safety expectations for edtech developers and suppliers to schools. This guidance will inform our decisions about what can safely be introduced to Pear tree students and when.

Use of staff devices within school:

Pear Tree permits authorised employees, including school staff, to use their personal mobile devices for approved administrative Pear Tree business and work purposes, including email, file sharing, and access to Pear Tree-deployed applications.

Important and school specific information includes:

- Any personal device must contain a level of security in line with our existing IT infrastructure; this will include passcode protection and automatic locking when idle.
- The Company accepts no responsibility for any loss or damage to personal devices that are the result of employee failure to observe rules, procedures or instruction, or, as a result of negligent behaviour.

- The Company may need to apply security policies to your device which will protect the Company's information held on your device. We expect you to accept any updates pushed to your device by the Company.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of Company and personal data due to operating system crash, errors, bugs, viruses, 166 malware, and/or other software or hardware failures, or programming errors that render the device unusable.

Photography and video recording of Students in Pear Tree School

At Pear Tree School we are committed to ensuring the safety and promoting the welfare of the children in our care and we expect staff to share the same commitment.

It is the policy of the school that photography or video recording of students, their work, or anything else which could identify a student is undertaken by school staff and residential staff only on devices owned by Pear Tree School. Photographs and video recording must be taken solely for the purpose of recording a child or a group of children participating in activities or celebrating their achievements as an effective form of recording their progression.

Student Device Use:

Pear Tree School Mobile Phone Policy:

Purpose:
This policy supports a calm, safe, and focused learning environment. While mobile phones can be useful tools, they can also cause distraction and safeguarding concerns. The school therefore sets clear expectations to ensure that technology enhances, rather than disrupts, students' learning and wellbeing.

In addition, for post-16 students, the policy acknowledges that mobile phones can play a role in promoting independence and improving personal safety when travelling to and from education independently. The rules below balance these benefits with the need to maintain a distraction-free school environment.

- Only students in Years 12 and 13 may bring mobile phones on to the school site.
- Students in all other year groups are not permitted to bring mobile phones to school.

Student responsibility:

- Any student in years 12 and 13 who arrives at school with a mobile phone must hand it in to reception on arrival.
- Any breach will result in the mobile phone being removed and returned to the student at the end of the school day. Home will be informed.
- No other devices of any kind are allowed in school such as smart watches or tablets. Any device that can capture any image is prohibited.

Mobile Data Access:
The school recognises that many young people now have unlimited and unrestricted access to the internet through personal mobile devices using mobile data networks such as 4G and 5G. Access via

mobile data is not subject to the school's filtering systems and therefore presents an additional safeguarding consideration. Such access may increase the risk of inappropriate or harmful use; the following may not be an exhaustive list:

- Sexually harassing peers through messages, social media, or image sharing.
- Self-generated intimate images consensually or non-consensually.
- Accessing, viewing, or distributing pornography
- Accessing or sharing other harmful, inappropriate, or illegal online content. The school acknowledges these risks and addresses them through clear behaviour expectations, safeguarding procedures, online safety education and appropriate consequences where necessary. Mobile phone checks are completed when concerns or vulnerability are identified.

Any incidents involving inappropriate online behaviour will be managed in line with the school's safeguarding and child protection procedures.

Cyber Awareness Plan: Pear Tree School

Purpose
Pear Tree School's Cyber Awareness Plan is designed to protect sensitive information, safeguard students and staff, and minimise disruption to education through effective cyber security measures, clear policies, comprehensive staff training, and age-appropriate student education.

Leadership and Governance
Pear Tree School protects all devices connected to school networks through appropriately configured boundary and software firewalls.

The Designated Safeguarding Lead (DSL) and Senior Leadership Team (SLT) undertake regular cyber security risk assessments and conduct termly reviews to identify vulnerabilities within hardware, software, systems, and data management processes.

The DSL compiles a termly safeguarding report for the Headteacher, highlighting any cyber security concerns, incidents, trends, or areas requiring improvement.

The DSL and SLT maintain strategic oversight of cyber security arrangements across the school. This includes ensuring that:

- Appropriate cyber security policies and procedures are in place.
- Staff receive relevant training and updates.
- Cyber security risks are regularly reviewed and mitigated.
- Leadership is accountable for maintaining cyber resilience and protecting school systems and data.

Staff Training

All staff with access to school IT systems and networks receive cyber security awareness training. Training includes:

- **A Guide to UK Data Protection**, delivered through Educare and refreshed every two years. This covers:
    - Personal data protection
    - Data security risks and challenges
    - Compliance with data protection legislation
- Cyber security awareness training provided by the National Cyber Security Centre (NCSC), including guidance on:
    - Recognising cyber threats
    - Protecting sensitive information
    - Safe online working practices
    - Reporting security concerns

Staff are regularly reminded that simple protective measures can significantly reduce cyber risks, including:

- Using strong and unique passwords
- Enabling multi-factor authentication where available
- Installing updates promptly
- Remaining vigilant to phishing attempts and suspicious activity
- Following the school's filtering and monitoring procedures

Student Education and Curriculum

Pear Tree School integrates online safety and cyber awareness throughout the curriculum to support pupils in becoming safe, responsible, and resilient digital citizens.

Pupils are taught age-appropriate knowledge and skills relating to:

- Basic use of laptops and digital devices
- Safe and effective use of search engines
- Creating and managing secure passwords
- Understanding e-safety and cyber security terminology
- Laws and responsibilities relating to online safety
- Safe online relationships and communication
- Digital resilience and managing online risks
- Social media safety and responsible online behaviour
- Identifying scams, phishing attempts, and misinformation
- Knowing how and when to seek help if concerned about online activity

Review and Monitoring:
This Cyber Awareness Plan will be reviewed annually by the DSL and SLT, or sooner in response to significant changes in guidance, legislation, technology, or cyber security threats.

Technical Safeguards:
Access Controls: In Pear Tree School we limit user privileges so that students, staff, and third parties only access the files and networks strictly required for their roles. Strict passwords are enforced at all times.

Cyber Incident Response Procedure:

Purpose:
Pear Tree School recognises that cyber incidents can affect the confidentiality, integrity, and availability of information and systems. A prompt and coordinated response is essential to minimise disruption, protect personal data, and safeguard students and staff.

What is a Cyber Incident?

A cyber incident may include, but is not limited to:

- Phishing emails or text messages.
- Malware or ransomware infections.
- Unauthorised access to school systems or accounts.
- Data breaches involving personal or sensitive information.
- Loss or theft of devices containing school information.
- Suspicious network activity.
- Compromised passwords or user accounts.
- Accidental disclosure of confidential information.

Reporting a Cyber Incident:

Any member of staff who suspects a cyber security incident must:

1. Immediately stop using the affected device or system if it is safe to do so.
2. Report the concern to the Headteacher, DSL, and IT Support without delay.
3. Preserve any relevant information, including screenshots, emails, or error messages.
4. Not attempt to investigate, delete files, or resolve the issue independently unless authorised.

Containment:

Upon notification, the Headteacher, DSL, and IT Support will assess the situation and take appropriate steps to contain the incident, which may include:

- Disconnecting affected devices from the network.
- Disabling compromised user accounts.
- Blocking malicious websites, email addresses, or applications.
- Restricting access to systems while investigations take place.

Assessment and Investigation:

The school's leadership team, in conjunction with IT support providers, will:

- Determine the nature and extent of the incident.
- Identify any affected systems, users, or data.
- Assess whether personal data has been compromised.
- Consider any safeguarding implications for students and staff.
- Maintain a record of actions taken and findings.

Communication:

Where appropriate, the school will:

- Inform relevant staff of any operational impact.
- Notify parents, carers, and external agencies where required.
- Consult with the Data Protection Officer regarding potential data breaches.
- Report incidents to the Information Commissioner's Office (ICO) where legally required.
- Seek advice from the National Cyber Security Centre (NCSC) where appropriate.

Recovery:

Following containment and investigation, the school will:

- Restore systems from secure backups where necessary.
- Change passwords and strengthen security controls.
- Verify that systems are safe before returning them to normal use.
- Monitor systems for any further suspicious activity.

Review and Lessons Learned:

Following any significant cyber incident, a review will be conducted by the Headteacher, DSL, SLT, and IT Support to:

- Identify lessons learned.
- Review the effectiveness of the response.
- Update risk assessments and procedures where necessary.
- Implement additional safeguards or training requirements.

All cyber incidents and actions taken will be recorded and retained in accordance with the school's safeguarding, data protection, and record-keeping procedures.

For further information - Please refer to Pear Tree School Data Protection Policy in Guidance and Good Practice Number 71 which highlights how to report any data breaches.

Appendix

Appendix A

Technology Agreement:
When I use the iPads or Laptops, I agree to be responsible, respectful, and safe.

Responsible

- I will only use the software that the teacher has asked me to use.
- I will safely and carefully get the devices and will sign out, close all apps and return the device when finished, making sure the device has been shut down appropriately.
- I will take care of the device and keep it away from food and drink.

Respectful

- I will only use the device at appropriate times.
- I will not be on the device when the teacher is talking, giving instructions or during a group discussion.
- I will not allow the device to distract me from learning.
- I will not use the device to record (pictures or videos) without consent.

Safe

- I will not use the device to search for inappropriate material.
- I will not change any settings, add, or remove apps.
- I will not take home any devices.
- I will let a teacher know if I see anything on the device that makes me feel uncomfortable or unsafe.

I understand that being able to use the devices during class time is a privilege; if I chose not to follow the above expectations, I am aware I may not be able to use the device.

References

Department for Education. (2025). *Generative artificial intelligence (AI) in education.* United Kindom: Department for Education. Available at: https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education (Accessed: 18/12/2025).

Department for Education. (2025). *Keeping Children Safe in Education 2025: Statutory guidance for schools and colleges*. United Kingdom: Department for Education. Available at: https://www.gov.uk/government/publications/keeping-children-safe-in-education (Accessed: 10/12/2025).

UK Council for Internet Safety. (2020). *Education for a Connected World: A framework to equip children and young people for digital life* (2020 edition). UK Government. Available at: https://www.gov.uk/government/publications/education-for-a-connected-world (Accessed: 19/10/2025).

Pear Tree Projects. (last updated: 2025). *Guidance and Good Practice. Policy document for the provision of care and education provided by pear tree projects.* United Kingdom.

ISS Guidance for Independent School Standards (April 2026)
DfE guidance August 2025
Data Protection Act 2018