PINEWOOD

Est. 1875

E-SAFETY

A Whole-School policy including the EYFS

Introduction

1. Pinewood recognises that internet safety is a whole school responsibility including staff, pupils and parents. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Children and young people may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. We therefore recognise our responsibility to educate our pupils, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies and how to mitigate risks, including but not limited to, the risk of theft, bullying, harassment, grooming, stalking, abuse and radicalisation. We also understand the importance of involving pupils in discussions about E-Safety and listening to their fears and anxieties as well as their thoughts and ideas.

Scope of this Policy

2. This Policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems.

3. This Policy as well as the Computer Resources (Acceptable Use) Policy for Pupils and the Computer Resources Policy for Staff cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

IT Equipment and Systems

4. The school has a well-equipped and well-attended Computer Suite and computers and mobile devices in various parts of the school which allow children monitored access to the Internet via a web filtering system. The school takes all reasonable precautions to limit exposure to harmful and inappropriate online material, whilst trying not to 'overblock' and impose unreasonable

restrictions on what our children can be taught. If pupils or staff discover an unsuitable or illegal website which has circumvented the filtering system it must be reported to the IT Network Manager.

Roles and Responsibilities

5. **The Governing Body.** The Governing Body of the school is responsible for the contents of this policy and for reviewing its effectiveness. The Governance Committee will review this policy at least annually on behalf of the Governing Body.

6. **Headmaster.** The Headmaster is responsible for the safety of the members of the school community and this includes responsibility for E-Safety. The Headmaster has delegated day-to-day responsibility to the Designated E-Safety Safeguarder and Head of Computer Science.

7. **Designated E-Safety Safeguarder/Head of Computer Science.** The **Designated E-Safety Safeguarder** and Head of Computer Science are responsible for ensuring that:

- Staff are adequately trained about E-Safety;
- Staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of E-Safety in connection to the school.
- All members of the school community comply with this Policy and work with the IT Network Manager to achieve this.
- Keep up to date on current E-Safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board (OSCP).
- The school have subscribed to 'National Online Safety' which is a website dedicated to keeping schools up to date with online safety. The website is able to offer up to date training at all levels, to staff as well as age appropriate resources for staff, pupils and parents about a wide variety of issues associated with online safety. The school is now a certified school in Online Safety and is working towards being certified in 'Safe Remote Education'.

8. **IT Network Manager.** The IT Network Manager is responsible for:

- Ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- Ensuring that the school meets the required E-Safety technical requirements and any relevant body E-Safety policy/guidance that may apply at the time.
- Ensuring that users may only access the networks and devices through a properly enforced password protection system.
- Keeping abreast with the rapid succession of technical developments.
- Training the school's support staff and teaching staff (in conjunction with the Head of IT) in the use of IT.
- Monitoring the use of the internet and emails, maintain content filters, and oversee the implementation of Smoothwall, software, which immediately notifies the DSL and Heads of

Year should inappropriate content/language be typed into a school IT system by a pupil, actioning immediate follow up.

9. **Staff.** All staff are required to sign the Computer Resources Policy for Staff before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any E-Safety issues which may arise in classrooms on a daily basis. All staff are aware that any abuse or suspected breach of E-Safety are to be raised to the DSL.

10. **Pupils.** Pupils are responsible for using the school IT systems in accordance with the Computer Resources (Acceptable Use) Policy for Pupils, and for letting staff know if they see IT systems being misused.

11. **Parents.** Parents are responsible for ensuring their child has read and understood the school's Computer Resources (Acceptable Use) for Pupils Policy.

Training

12. **Staff: Awareness and Training**. All staff required to use the School's IT systems receive IT Induction Training on arrival as required from the Director of Studies. Further E-Safety training is provided on a regular basis as part of Safeguarding Training and other Inset Training as coordinated by the DSL.

13. **Pupils: E-Safety in the Curriculum**. Pinewood recognises the need to ensure children are safeguarded from potentially harmful and inappropriate online material, acknowledging that this now explicitly includes misinformation (including fake news) and conspiracy theories, reflecting growing risks in the digital space. Pupils are made aware through E-Safety sessions, as well as Computer Science lessons, of the benefits, as well as the risks, of using internet connected devices and how they can protect themselves online, both through their conduct and how they interact with others; they are also made aware of what to do if they have any concerns and who they should speak to.

Further details are covered under the curriculum policies. Cyberbullying and sexting by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures. More information can be found in the Cyberbullying and Computer Resources (Acceptable Use) for Pupils Policy.

14. **Parents**. The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school. The school regularly provides up to date and important E-Safety information to parents.

Electronic Provision

15. **Email.** Pupils can contact staff internally; however, they are restricted from emailing each other and external email addresses. Weekly boarders are permitted to email their parents/relatives during boarding times, with other boarders having email access by request. Pupils must never reveal any personal details or arrange to meet anyone without specific permission. E-mails should only be opened from known senders, and attachments should only be opened if expected; otherwise, all emails and attachments should be treated as suspicious and should not be opened. Pupils must report any suspicious, abusive, offensive or inappropriate emails immediately.

16. **Video Calls.** Boarding children with parents overseas may be allowed to video call on specifically set-up computers. Certain departments have links with an overseas school – Shonda for instance – and Pinewood recognises there is much to be gained from live interaction with pupils abroad to further cultural tolerance and understanding. Contact should be confined to the classroom, only made with children of similar age, always under staff supervision, of an educational nature, and Christian names only should be used.

17. **Use of Mobile Technology.** We are aware of the ever-increasing sophistication of technology and the ability for small gadgets to possess enormous capability, which means we have to be vigilant as to what our children can and cannot bring to school. Therefore, no child should bring any other gadgets/devices (including mobile phones, smartphones, smart watches, tablets and handheld devices) to school except in the case of boarders, when a basic radio or a screenless iPod (Shuffle) or equivalent may come in. Nothing that is capable of 'streaming' or is able to access or share access (as a hotspot) to the web through wireless, 3G or 4G (including dongles) is acceptable. Only basic models of Kindle or equivalent e-Readers can come to school and we retain the right to monitor their content.

18. **Other Devices.** On no account should portable gaming devices or portable DVD players be brought to school. Cameras are really only needed for out of school trips and should never be used without permission. We are happy that parents use cameras in the school grounds and in the theatre and sports hall. Laptops for specified children are allowed but only for use as 'word processors'. They are issued by the school and remain school property. They are not for 'free-time' use, i.e. games and films. Our IT resources also give the children, especially boarders, the chance to play some suitable games. The school possesses DVD players, and suitable films and videos are available to boarders in the evening when appropriate. In addition, the school has games consoles which pupils may be allowed to use from time to time.

19. **Prevent Duty.** The School has a responsibility to ensure that children are safe from terrorist and extremist material when accessing the internet in School and hence suitable filtering is in place. More generally, the School uses its normal routes to help equip the pupils to stay safe online, both in school and outside. Further details can be found in the School's Prevent Policy.

20. **Staff should have regard for the following related policies:**

Computer Resources (Acceptable Use) for Pupils
Computer Resources (Acceptable Use) for Staff
Anti-Bullying Discipline & Rewards
Cyber-bullying
Social Media
Twitter and Instagram
Data Protection
Safeguarding (Child Protection)
Prevent
AI Policy

Reviewed by: Angela Kirby, Head of Computer Science
Review Date: September 2026
Next Review Date: September 2027

Reviewed and approved by: Governance Committee
Review Date: September 2025
Next Review Date: September 2026