



ONLINE SAFETY POLICY SEPTEMBER 2025

Policy Originator: Online Safety Lead

Status: Non-statutory **Review Period:** 3 Years

Date: September 2025 **Next review date:** September 2028

Online Safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for **behaviour and anti-bullying, safeguarding, staff code of conduct, acceptable use policy for visitors,, data handling and photography.**

This Policy applies to all members of the school community – including staff, pupils, volunteers, parents/carers, visitors, and community users – who access or use the school's digital technology systems, whether on or off school premises.

This policy is informed by and adheres to the following key documents:

- Keeping Children Safe in Education (KCSIE) – DfE
- Working Together to Safeguard Children – DfE
- Teaching Online Safety in Schools – DfE
- The Prevent Duty – DfE
- Ofsted Education Inspection Framework (EIF)
- General Data Protection Regulation (GDPR) and Data Protection Act 2018
- Sexual violence and sexual harassment between children in schools and colleges – DfE
- Generative Artificial Intelligence (AI) in Education - DfE

Leadership and Management of Online Safety Roles and Responsibilities

- **Designated Safeguarding Lead (DSL)** – Michelle Dutton (Headteacher) - overarching responsibility for online safety.
- **Deputy Designated Safeguarding Lead (DDSL):** Gemma Thorne (Computing Lead & EYFS Leader)
- **Online Safety Leader:** Gemma Thorne (Computing Lead & EYFS Leader)
- **Headteacher and Senior Leadership Team (SLT)** – Michelle Dutton (Headteacher), Helen Radley (SENCO) and, Gemma Thorne (EYFS Leader) -strategic oversight.
- **Governing Body** – ensuring appropriate policies and resources are in place.
- **Staff** – understanding and embedding online safety into teaching and behaviour management.
- **Pupils** – knowing their rights and responsibilities online.
- **Parents and Carers** – supporting the school's approach at home.
- **ICT/Technical Support Staff** – James Peers, implementing filters, monitoring systems and platform security.

Using this policy

Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been approved by governors.

The online safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones and tablets.

The online safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

1. Introduction

In line with current expectations the school has a computer system which gives the children access to the Internet.

Usually, the resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times, they will be able to move beyond these, to sites unfamiliar to the teacher.

The problems and issues that have been highlighted by the media concern all schools. Whilst some of the media interest is hype, there is genuine cause for concern that children might access unsuitable material accidentally.

The purpose of this policy is to:

- Establish the ground rules we have in school for using the Internet
- Describe how these fit into the wider context of our discipline and PSHCE policies
- Demonstrate the methods used to protect the children from sites containing pornography, racist or politically extreme views and violence.

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

We feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

2. Teaching & Learning

The Internet is an essential element in 21st century life for education, business, and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience.

Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be taught about online commercial risks, including advertising and marketing, so that they can recognise and manage these safely.

2a. Remote Learning

While most learning takes place on site, there may be occasions when children are required to learn at home (for example, due to illness or school closure). It is important that online safety standards remain consistent, so children continue to be protected and supported when accessing education remotely.

When children are learning at home, the same principles of online safety apply as in school. We will:

- Ensure parents and carers know what their child is being asked to do online, including which sites they will be accessing and which staff will be interacting with them.
- Remind parents and carers of the importance of supervising their child's online activity and of supporting them to stay safe online.
- Make sure that school systems used for remote learning are subject to the same filtering and monitoring as when accessed on site, wherever possible.
- Provide parents and carers with guidance on keeping children safe online during periods of home learning.

3. Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform online policy.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- Physical monitoring of the internet by staff will ensure children are accessing appropriate content.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

4. Pupils access to the Internet

Our school uses RM as the internet provider and their age-related filtering system, which will minimise the chances of pupils encountering undesirable material. Any school will normally only allow children to use the Internet when there is a responsible adult present to supervise, however, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer/smartboard/ipad screen.

Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils the expectation we have of pupils.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use – child friendly search engines will be used for children to search the internet e.g. www.safesearchkids.com.
- Pupils will be taught how to report unpleasant Internet content
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

- Pupils will be shown how to publish and present information appropriately to a wider audience without giving out personal details or information which may identify them.

5. Expectations of pupils using the Internet

- At Shalford Infant & Nursery School we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally they are expected to report it immediately to a teacher or teaching assistant, so that the Service Provider can block further access to the site.
- Pupils must ask permission before accessing the Internet and before printing anything material which they have found.
- Computers and tablets should only be used for schoolwork, unless permission has been granted otherwise.
- At Foundation Stage and Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials
- Complaints of internet misuse will be dealt according to the school behaviour and anti-bullying policy. Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures. Pupils and parents will be informed of consequences and sanctions for pupil's misusing the internet and this will be in line with the school's behaviour and anti-bullying policy.
- Appropriate elements of the online safety policy will be shared with children.
- Online safety rules will be posted in all networked rooms.
- Children will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of online safety issues and how best to deal with them will be provided for children through the Computing and PHSE curricula.
- To apply our School Rules when online: Ready, Respectful, Safe when accessing the Internet.

| Ready | Respectful | Safe |
|---|--|--|
| <ul style="list-style-type: none"> • Be ready to use the internet in a safe and helpful way. • Always use passwords to keep your accounts safe. | <ul style="list-style-type: none"> • Be kind to others when using the internet. • If you see something unkind or not right online, tell a trusted adult. | <ul style="list-style-type: none"> • Never share personal details, like your address or phone number, online. • If something makes you feel uncomfortable or you see something strange, tell a grown-up straight away. |

6. Monitoring

All online safety incidents will be recorded and tracked using CPOMS, ensuring that appropriate actions are taken to protect children and staff while also informing the online safety policy. As a comprehensive safeguarding tool, CPOMS monitors online safety alongside other safeguarding and behaviour concerns.

The school is committed to taking all reasonable measures to ensure online safety for all users. However, it acknowledges that incidents may occur both inside and outside the school that require intervention. To address this, the school will ensure:

- Clear reporting procedures are established, understood, and followed by all members of the school community.
- All members of the school community receive appropriate training and guidance on recognising, reporting, and responding to online safety concerns.
- Online safety concerns are addressed promptly, with appropriate support provided to those affected.
- Online safety policies and procedures are regularly reviewed and updated in response to emerging risks and incidents.

6a. Online Safety Incident Process

Purpose

To ensure that all online safety concerns are handled promptly, consistently, and effectively, protecting children, staff, and the school community. This process clarifies how online issues are identified, how staff should intervene, and how incidents are escalated when necessary.

Step 1: Identification of Concerns

Online safety concerns may be identified through:

- **Pupil reports:** Children reporting inappropriate content, cyberbullying, or other online incidents.
- **Staff observation:** Teachers or support staff noticing unsafe use of devices, concerning online behaviour, or breaches of policy.
- **Monitoring systems:** Alerts from school internet filters, network monitoring software, or CPOMS notifications.
- **Parental reports:** Concerns raised by parents about online safety at home that affect school learning or wellbeing.

Step 2: Immediate Intervention

Staff are expected to act promptly to safeguard the child or others involved:

- Stop the inappropriate activity immediately if it is occurring in school.
- Confiscate or secure the device if necessary.
- Reassure children affected and remove them from any immediate risk.
- Record initial observations and actions factually in CPOMS.

Step 3: Escalation

All online safety incidents are escalated according to severity and safeguarding implications:

- **Minor incidents:** Handled by class teacher or supervising adult; recorded on CPOMS; parents informed if appropriate.
- **Moderate incidents:** Reported to the Designated Safeguarding Lead (DSL) for review and follow-up.
- **Serious incidents or safeguarding concerns:** Immediate escalation to the DSL and Headteacher. The DSL will follow school safeguarding procedures and liaise with external agencies if required (e.g., police, social services).

Step 4: Investigation and Follow-Up

- The DSL or appointed staff member will investigate incidents thoroughly and proportionately.
- Evidence may be collected from devices, screenshots, or witness accounts.
- Appropriate support will be provided to children or staff affected, including reassurance, guidance, or counselling.
- Parents/carers will be informed as appropriate, in line with safeguarding guidance.

Step 5: Recording and Monitoring

- All incidents must be logged on CPOMS, including actions taken and outcomes.
- Patterns or repeated incidents are reviewed by the Online Safety Lead and SLT to inform updates to policy, teaching, or monitoring practices.
- Staff responsible for monitoring will ensure incidents are analysed to improve prevention measures.

Step 6: Prevention and Education

- Lessons in Computing and PSHE will reinforce safe and responsible use of technology.
- Staff will receive ongoing training to recognise, report, and respond to online safety concerns.
- Parents/carers will be provided with guidance to support safe online use at home.

7. Social networking & personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved

- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils

8. Staff use of the Internet

It is important that teachers and support staff are confident enough to use the Internet in their work. The School Online Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

Abuse of the Internet or email by any school employee is a serious matter that could result in disciplinary procedures. Email sent via the school proxy server is monitored for inappropriate content and attachments. If staff have doubts as to the legitimacy of any aspect of their Internet use in school they should discuss this with their line manager to avoid any possible misunderstanding.

All staff, including administration, premises manager, governors and helpers should be included in appropriate awareness raising and training annually. Internet use should be included in the induction of new staff.

All staff, including teachers, supply staff, teaching assistants and support staff should read the School Online Safety Policy and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

9. Home usage & parental support

Internet use in pupils' homes continues to increase rapidly and many pupils have unrestricted access to the Internet at home. The school aims to help parents plan appropriate, supervised use of the Internet by helping them to understand more about online safety themselves via online safety workshops for parents and regular online safety information via the school newsletter. Details of sites offering support and guidance on home Internet use are available on the school website. Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters and on the school web site.

10. How will ICT system security be maintained?

The school ICT systems will be reviewed regularly with regard to security. Strategies will be discussed with the Learning Partners Academy Trust, particularly where relating to the wireless network, firewall configurations and anti-virus software.

- All users must act reasonably. Loading non-approved software could cause major problems. Good password practice is required including logout after use
- Cabling should be secure and wireless LANs safe from interception
- Servers must be located securely and physical access restricted
- The server operating system and Microsoft Sharepoint must be secured to a high level
- Virus protection for the whole network must be installed and current (this must include arrangements for teacher laptops to be periodically updated)
- The network manager will ensure that the system has the capacity to take increased traffic caused by Internet use
- If staff or pupils come across unsuitable online materials, the site must be reported to the Online Safety Lead
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

11. School website and Social Media

- A website can promote the school and link to other good sites of interest.
- The point of contact on the Website should be the school address, school email and telephone number. Staff or pupils' home information will not be published.
- Written permission will be obtained from parents or carers before photographs, names or work of pupils are published on the school website or any school-run social media, as set out in Surrey Safeguarding Children Board Guidance on using images of children.
- Pupils' full names will not be used anywhere on the website or on social media, and particularly not associated with photographs. Parents or carers will have the opportunity to opt out of publication of photographs of their children on the school website at the point of enrolment.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

12. Email use in school

- Pupils and staff may only use approved e-mail accounts on the school system.
- Only school approved email accounts should be used for email by pupils. This will only occur under direct supervision by an adult and as part of a directed task.
- All communication between staff and pupils or families will take place using school equipment and/or school accounts. Families will be contacted via email using the My Child at School app (MCAS).
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Where referring to pupils in emails, initials should be used in the subject heading.
- Incoming e-mails should be treated as suspicious and attachments not opened unless the author is known. Staff to pupil email communication must not take place.
- Emails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. The forwarding of chain messages is banned. In the school context, email should not be considered private and the school and the Learning Partners Academy Trust reserve the right to monitor email.

13. Mobile phone and handheld device use in school

- Mobile phones and personally owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- Mobile phones and personally owned devices must not be used during lessons or formal school time. They should be switched off or set to silent and kept securely stored, out of sight. Bluetooth communication should be disabled or set to hidden.
- If a staff member is expecting a personal call which is urgent and needs to be answered they may leave their phone with the School Office to answer on their behalf or seek specific permissions to use their phone outside of break times or after school.
- Staff use of mobile phones during the school day will normally be limited to the lunch break and after school. The school reserves the right to search the content of any mobile or handheld device on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or handheld devices may be searched at any time as part of routine monitoring.
- All visitors to school are requested to keep their phones on silent.

- Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties such as contacting pupil's parents, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- No pupils should bring his or her mobile phone or personally owned device into school. Any device brought into school will be confiscated.

14. Use of Smartwatches in School

The school recognises that smartwatches are increasingly common among both children and staff. While they can be useful for telling the time, tracking fitness, and supporting communication, safeguarding, privacy, and minimizing distractions are the school's highest priorities. Clear expectations are set to ensure that smartwatches are used safely and appropriately, supporting children's wellbeing and learning.

Children

- Children may wear simple watches or fitness trackers that only tell the time or count steps.
- Smartwatches with cameras, internet access, messaging, or recording functions must not be used in school.
- If a child misuses a watch, it will be removed and returned to parents or carers at the end of the day.
- Parents and carers are asked to check their child's device to ensure it is suitable for school use.

Staff

- Staff may wear smartwatches in school but must act as positive role models in their use.
- Smartwatches must not be used to take photographs, record audio, or access the internet while working. Notifications should be muted during lessons and when supervising children to avoid distraction.

Any use of smartwatches must comply with the school's safeguarding, data protection, and acceptable use policies.

15. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998
- Should any pupils encounter any offensive materials online accidentally they are expected to report it immediately to a teacher or teaching assistant, so that the Service Provider can block further access to the site.
- The Teacher or Teaching assistant should record the incident on the school's safeguarding system, CPOMS, which is then reviewed by the designated Safeguarding Lead. Relevant parents will be informed. All incidents are monitored by a member of the Senior Leadership Team.
- The Headteacher and DSL should use the flow chart (Appendix 3) along with the screening tool and the Surrey Child Protection Procedures to determine next steps in supporting the child involved in the incident. Schools' DSL will be conversant with these and the processes for referral.
- Should any pupils encounter any cyber bullying by other pupils in the school, this should be recorded on CPOMS by the staff member to which the information was disclosed, in line with our Anti-Bullying Policy.
- The Designated Safeguarding Lead will inform the head teacher/deputy head of the incident recorded on CPOMS.
- The headteacher will interview all concerned and will add further action to CPOMS.
- Class teachers and support staff (as appropriate) will be kept informed.
- Parents will be kept informed.
- Appropriate disciplinary action will be taken.

- The log of online incidents will be monitored and reviewed regularly to ascertain whether any changes need to be made, e.g. to the school's online safety policies, anti-bullying policies, training, curriculum content.

16. Using Artificial Intelligence (AI)

- **Responsible Use:** When using AI tools and technologies, it is important to ensure they are used in a responsible and ethical manner. Users should always be mindful of the content they interact with and share, ensuring it aligns with the school's rules and values of safety, respect, and responsibility.
- **Data Privacy:** AI tools may collect and process data to function effectively. It is essential that any personal information should not be entered or shared through AI tools. The school will ensure that AI tools comply with relevant data protection laws and safeguard the privacy of all users.
- **Monitoring and Content:** AI-generated content, such as text, images, or recommendations, must be carefully monitored for accuracy and appropriateness. AI should not be used to generate harmful, inappropriate, or misleading content. Teachers and staff are responsible for guiding pupils in identifying and questioning AI-generated content.
- **AI in Education:** AI tools used for educational purposes should enhance learning and support student development. However, pupils should be aware that AI may not always provide correct or complete information. It is important for pupils to verify information from reliable sources.
- **Age Restrictions:** When using AI tools in the classroom, we will comply with age restrictions to ensure that students are only exposed to appropriate content and tools that align with their developmental stage.
- **Reporting Concerns:** If a pupil, staff member, visitor or parent encounters any concerns or issues with AI tools, including the use of AI inappropriately or in an unsafe manner, they should report it to the school's DSL.

17. Authorising Access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians, and governors) must read this policy and sign to declare compliance with it before accessing the school's IT systems.
- Individuals not employed by the school must read and agree to follow the acceptable use policy before being given access to the internet via school equipment.

18. Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international nature and interconnectedness of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC (Surrey County Council) can accept liability for material accessed or any consequences resulting from internet access.

19. Handling Online Safety Complaints

- Complaints of internet misuse will be addressed according to the school's behaviour policy.
- Complaints of a child protection nature must be handled in accordance with the school's child protection and safeguarding procedures.
- Pupils and parents will be informed of the consequences and sanctions for internet misuse, in line with the school's behaviour policy.
- Incidents involving online safety will be logged and tracked on **CPOMS**.

20. Communication of the Policy

To Pupils

- Pupils will be regularly reminded about the content of the **Online Safety Guidelines** as part of their ongoing online safety education.

To Staff

- All staff will be shown where to access the **Online Safety Policy** and its importance will be explained.

- All staff must sign and agree to comply with this policy in order to gain access to the school's IT systems and the internet.
- All staff will receive online safety training on an ongoing basis.

To Parents

Parents and carers will be updated with online safety information in newsletters and will have access to the policy through the school website.

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff and visitors are aware of their responsibilities when using any form of ICT. All staff and visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Online Safety Leader.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, smart watches, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email / Internet / network and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will ensure that all electronic communications with parents and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.
- I will not install any hardware or software without the permission of the IT technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without the permission of the parent/carers, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will report any incidents of concern regarding children's safety to the Online Safety Leader, a Designated Safeguarding Lead or the Headteacher.
- I will ensure that electronic communications with pupils, parents and ex-pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will support the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure my school laptop (where applicable) has a secure password on it. I will only use an encrypted USB pen.
- I will not use my own camera to take photos of children and I will not store/download any photos of children at my house on other devices or storage systems



ICT Acceptable Use Policy for Visitors **September 2025**

All visitors to Shalford Infant & Nursery School must adhere to our Acceptable Use Policy for visitors. This policy covers email, the internet and mobile devices, including smart watches.

If you do not understand anything in this policy, please ask for clarification.

- ⊘ Mobile phones and other mobile devices are not allowed to be used on the school site. Smart watches must not be used for any other use than telling the time.
- ⊘ Photographs or videos of pupils must not be captured by parents or visitors on the school site, without the express permission of the Headteacher.
- ⊘ If granted permission to capture images of pupils, the images must not be shared (i.e. on social media) if they clearly show any pupil other than your own child.
- ⊘ Access to the school WiFi will not be granted to visitors. Requests to access the Guest WiFi will be considered based on visitor activities.
- ⊘ Visitors who are granted access to our ICT network must not look at inappropriate materials such as pornography or extremist materials.
- ⊘ If you witness anyone capturing images of a pupil at an inappropriate or not-permitted time, please report this to one of the Designated Safeguarding Leads immediately.

Responding to an Online Safety Concern

