



E-SAFETY POLICY

Priestley Smith Specialist VI School

September 2026

Policy review date: September 2027

Policy status: Statutory

Responsible member of SLT: Liz Clabon Deputy Headteacher

Priestley Smith School is committed to the rights of the child as outlined in the UN Convention and is working towards Rights Respecting Schools Gold award. This belief influences everything the school does and impacts upon all our policies.

Article 3 The best interests of the child must be a top priority in all things that affect children.

Article 16 Every child has the right to privacy. The law should protect the child's private, family and home life, including protecting children from unlawful attacks that harm their reputation

Article 17 Every child has the right to reliable information from a variety of sources, and governments should encourage the media to provide information that children can understand. Governments must help protect children from materials that could harm them

Article 23 A child with a disability has the right to live a full and decent life with dignity and independence, and to play an active part in the community.

This policy has been updated with regard to Keeping Children Safe in Education 2026 (KCSIE), current Department for Education online safety guidance and the DfE filtering and monitoring standards. It should be read alongside the school Safeguarding and Child Protection Policy, Behaviour Policy, Data Protection Policy, AI Policy and relevant Acceptable Use Agreements.

1. Introduction

1.1 The governing body of Priestley Smith School has adopted this policy to help the school meet its responsibilities for safeguarding and educating children, for regulating the conduct of employees and for complying with legislation covering the use of information and communication technologies and digital and mobile devices.

1.2 This policy will be reviewed at least annually by the school and governing body, and sooner where there are changes to statutory guidance, safeguarding risks, technology or the school's filtering and monitoring arrangements.

2. Basic principles

2.1 The governing body recognises that safeguarding children online is an integral part of safeguarding. In accordance with KCSIE 2026, the school takes a whole-school approach to online safety and ensures that appropriate policies, procedures, education, filtering and monitoring are in place and reviewed regularly.

2.1a Online safety risks are considered within four broad areas: content (what pupils may see or be exposed to), contact (who they interact with), conduct (how they behave online) and commerce (risks such as scams, advertising and financial exploitation).

2.2 The policy applies to all members of the school community, including staff, pupils, volunteers, parents and carers, governors, visitors and community users who have access to, and are users of, the school's Information and Communication Technology systems or who use their personal devices in relation to their work at the school.

2.3 The governing body expects the Head Teacher to ensure that this policy is implemented, that training in e-safety is given high priority across the school, that consultations on the details of the arrangements for e-safety continue with all employees on a regular basis, and that any necessary amendments to this policy are submitted to this governing body for approval.

2.4 The principal context for this policy is safeguarding children. It will be applied alongside the school Safeguarding and Child Protection Policy and current local safeguarding partnership procedures. Online safety concerns will be managed as safeguarding concerns where appropriate.

2.5 The governing body expects the Head Teacher to arrange for this policy to be published to all employees and volunteers in the school and for necessary instructions and guidance, particularly on acceptable use, to be given to pupils in a manner suited to their ages and abilities.

3. Roles and responsibilities

Governing body

3.1 The governing body has overall strategic responsibility for online safety and for ensuring that appropriate filtering and monitoring systems are in place. It will ratify and review this policy at least annually, receive assurance about the effectiveness of filtering and monitoring, and ensure that identified actions are addressed.

3.2 Governors are responsible for ensuring that proper procurement procedures are used if they decide to purchase information technology services from an external contractor and that City Council or other reputable specialist advice is taken on the specification for those services to ensure proper security and safeguarding of children.

Head Teacher

3.3 The Head Teacher is responsible for ensuring that

- the governing body is offered appropriate support to enable this policy and its application to be reviewed regularly, and to ensure that other school policies, including that on pupils' behaviour, take account of this e-safety policy;
- the governing body is given necessary advice on securing appropriate Information and Communication Technology systems;
- the school obtains and follows City Council or other reputable guidance on Information and Communication Technology to support this policy;
- the Designated Safeguarding Lead (DSL) has lead responsibility for safeguarding and online safety, including understanding the school's filtering and monitoring arrangements, reviewing relevant reports and responding to safeguarding concerns identified through those systems;
- there is effective consultation with all employees, and other users of the school's Information and Communication Technology systems, to take account of the particular features of those systems and educational, technical and administrative needs;
- the school provides all staff with safeguarding and online safety training at induction and regular updates thereafter. Staff will understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring and know how to report online safety concerns;
- pupils are taught online safety as part of a broad and balanced curriculum, in an age-appropriate, developmentally appropriate and accessible way;
- the senior leadership team is aware of the procedures to be followed in the event of a serious e-safety incident, including an allegation made against an employee, and that all employees know to whom they should report suspected misuse or a problem ;
- records are kept of all e-safety incidents and that these are reported to the Senior Leadership Team;
- necessary steps have been taken to protect the technical infrastructure and meet technical requirements of the school's Information and Communication Technology systems;
- there is appropriate supervision of, and support for, technical staff, including technical services and Askelite technicians.
- any outside contractor which manages Information Technology for the school undertakes all the safety measures which would otherwise be the responsibility of the school to the standard required by the school and is fully aware of this policy and that any deficiencies are reported to the body which commissioned the contract.

Other employees

3.4 Other employees are responsible for

- undertaking such responsibilities as have been delegated by the Head Teacher commensurate with their salary grade and job descriptions;
- participating in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum;
- using Information and Communication Technology in accordance with this policy and the training provided;
- reporting any suspected misuse or problem to the person designated by the school for this purpose.

Pupils

3.5 Pupils are expected to use Information and Communication Technology systems and devices in accordance with their appropriate acceptable use policy, the school's behaviour policy and the instructions given to them by staff.

Other users

3.6 Volunteers, including governors, who help in the school and who use Information and Communication Technology systems and devices in helping the school are expected to

- participate in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum;
- use Information and Communication Technology in accordance with this policy and the training provided;
- report any suspected misuse or problem to the person designated by the school for this purpose.
- Be aware of and sign to show their agreement to abide by the terms of the acceptable use policy for staff, governors and visitors.

Parents

3.7 Parents who help in the school as volunteers are covered by 3.6 above. Parents who are not voluntary helpers in the school are nonetheless subject to the law in the event of misuse of Information and Communication Technology.

Visitors

Visitors to the school are expected to follow the procedures set out in the current Visitors to School Policy. If during the course of their visit they need to use school ICT systems, they must first be made aware of the content of this eSafety policy and comply with its terms, as consistent with their role while visiting the school.

4. Acceptable use

4.1 The use of Information and Communication Technology should follow the following general principles:

- This policy should apply whether systems are being used on or off the school premises.
- The school's Information and Communication Technology systems are intended primarily for educational use and the management and administration of the school. During work breaks appropriate, reasonable personal use is permitted.
- Data Protection legislation must be followed.
- Users must not try to use systems for any illegal purposes or materials.
- Users should communicate with others in a professional manner.
- Users must not disclose their password and they should not write it down or store it where it is possible that another person might steal it. Users must not attempt to use another person's user-name or password. A secure record of passwords may be kept for any student with recall and/or memory difficulties.
- Users must report as soon as possible any apparently illegal, inappropriate or harmful material or event to the Headteacher.

4.2 Acceptable Use Policies

A number of acceptable use policies are attached to this policy and will form part of it.

- Specific acceptable use policies are provided for Foundation Stage, Primary (KS1 & 2) students, Secondary (KS3,4 & 5) students and staff and other adults.
- At the start of each academic year a copy of the appropriate acceptable use policy will be sent home for the information of parents/carers and pupils will sign to show their agreement to be bound by the terms of the policy. The terms of the acceptable use policy will be explained verbally to foundation stage pupils (and any others where this is the most appropriate method of communicating the agreement).
- Similarly at the start of each academic year staff and other adults to whom it may apply will sign a copy of the staff acceptable use policy. Depending upon the nature of their visit, visitors may need

to be made aware of the appropriate use policy, and if making use of school computer facilities, sign to show their agreement.

- Key stage leaders will keep records to show pupils' agreement to be bound by the appropriate acceptable use policy. Similar records for staff and other adults will be kept within the existing staff confidential records.

4.4 Personal devices, mobile technologies, school-managed devices used away from school, cloud services, messaging, social media, livestreaming and other online services must be used in accordance with the school's safeguarding, behaviour and acceptable-use expectations. Any separate school policy on mobile phones or personal devices also applies.

- Although pupil and student acceptable use policies are differentiated by Key Stage as above the individual development of pupils may suggest that a policy from a different key stage may be more appropriate for an individual pupil. In these cases the Key Stage Leader should keep a record of the particular policy that an individual pupil has agreed to be bound by, verbally or by signing.

4.3 Use of social media networks or sites, whether by pupils or employees, should be subject to the same standards as the school would expect for behaviour and conduct generally (as set out in the school's code of conduct). The school accepts the separation of private life and work and will not concern itself with people's private lives unless it appears that the law has been broken, or that an employee is in breach of contract, or that the school is, or will be, brought into disrepute.

5. Education and training

5.1 Education and training in online safety will be given high priority across the school and will reflect current safeguarding risks, pupils' age, developmental stage, visual impairment, SEND and communication needs.

5.2 Online safety education will address the four broad areas of online risk identified in KCSIE: content, contact, conduct and commerce. Teaching will be embedded across relevant curriculum areas and will help pupils recognise, assess and manage online risk, seek help and report concerns. The school's separate AI Policy governs the use of artificial intelligence and generative AI.

5.4a Staff training and updates will include relevant emerging online harms, the school's filtering and monitoring arrangements, how to recognise online safeguarding concerns and the procedures for reporting them to the DSL or deputy DSL.

5.3 The school will offer education and information to parents, carers and community users of the school about e-safety.

5.4 Suitable training will be provided through the school for all employees, as part of induction and subsequently during their employment in the school. There will be a regular review of the training needs of all staff and the content of training should be kept up to date. The training will be linked to training about Child Protection and Data Protection. It will cover related matters such as the law on Copyright of electronic materials.

5.5 Volunteers and governors who use Information and Communication Technology during their work will be offered the same training as employees.

6. Data Protection

6.1 The school will ensure that its technology systems and processing of personal data comply with current UK data protection legislation and the school Data Protection Policy. Access to monitoring information will be restricted to authorised staff and handled lawfully, proportionately and transparently.

7. Technical aspects of e-safety

7.1 The school will provide a safe digital and online environment through appropriate technical controls, cyber security, filtering and monitoring arrangements, informed by current DfE standards and the school's safeguarding risk profile.

7.2 The governing body has overall strategic responsibility for ensuring appropriate filtering and monitoring. The provision will be formally reviewed at least once every academic year by appropriate

members of SLT, the DSL, IT support and the responsible governor. The review, findings and actions will be recorded. Additional checks will be undertaken at a frequency informed by the school's context and risk assessment.

7.3 Filtering and monitoring arrangements will take account of pupils' age, visual impairment, SEND, communication needs and other vulnerabilities. Systems must support accessibility and teaching and learning while reducing access to illegal, inappropriate and potentially harmful content.

7.4 Filtering will apply appropriately to school-managed internet-connected devices and services, including devices used off-site where technically possible. The school will understand the coverage and limitations of its filtering arrangements and will take reasonable steps to mitigate identified limitations. Filtering will not unreasonably restrict legitimate teaching, learning or accessibility resources.

7.5 Monitoring will be effective and proportionate to the safeguarding needs of the school. Relevant alerts and reports will be reviewed by appropriately trained and authorised staff. Safeguarding concerns identified through monitoring will be reported promptly to the DSL or deputy DSL, acted upon in accordance with safeguarding procedures, and outcomes recorded. IT support will maintain systems, undertake agreed checks and provide appropriate reports.

7.6 All staff will be made aware of the school's filtering and monitoring arrangements, their role in safeguarding pupils online, and how to report concerns. The school will consider filtering and monitoring implications when introducing new devices, services or technologies. The use of AI is addressed in the school's separate AI Policy.

8. Dealing with incidents

8.1 Any online safety concern relating to possible abuse, neglect, exploitation or other safeguarding harm must be reported without delay to the DSL or deputy DSL and managed in accordance with the school Safeguarding and Child Protection Policy and KCSIE. Staff should not delay action while attempting to investigate the matter themselves.

8.2 Any suspicions of other illegal activity should be reported to the Headteacher or Chair of Governors, who will then follow the current school procedures for allegations involving pupils, staff, other adults or the Headteacher as appropriate.

8.3 Suspicions of inappropriate, as distinct from illegal, use of Information and Communication Technology should be reported to the Head Teacher or other designated member of the Senior Leadership Team for investigation and appropriate action. This may lead to informal management discussions, improved training or, depending on the nature of the alleged misuse, investigation under the disciplinary procedure for employees, or the school's behaviour policy for pupils.

Recognising and reporting suspicious emails, messages and online activity:

- Users should not rely on the sender name, email domain, use of their name, branding or appearance of a message as proof that it is genuine.
- Be cautious about unexpected links, attachments, QR codes, requests for passwords or authentication codes, unusual payment requests, urgent demands, and unexpected changes to bank or contact details.
- Where a message is unexpected or sensitive, verify it through a separate trusted method before acting. Do not use contact details supplied only within the suspicious message.
- Suspicious messages, phishing attempts, compromised accounts and other cyber-security concerns must be reported promptly in accordance with the school's reporting procedures. Where a concern may involve safeguarding, it must also be reported to the DSL or deputy DSL.

Foundation Stage Acceptable Use Agreement / e-Safety Rules

This is the information that needs to be passed on to pupils verbally

These images or similar ones may be enlarged or tactile equivalents produced to help understanding.



I will only use computers and other ICT equipment when I am with an adult.

I will always take care of ICT equipment and computers and be sensible when using them.



If I see something on the computer which is nasty or makes me unhappy I will tell my teacher straight away.

Primary Student Acceptable Use Agreement / e-Safety Rules

These rules will almost certainly need to be discussed with the pupil before they can be agreed.

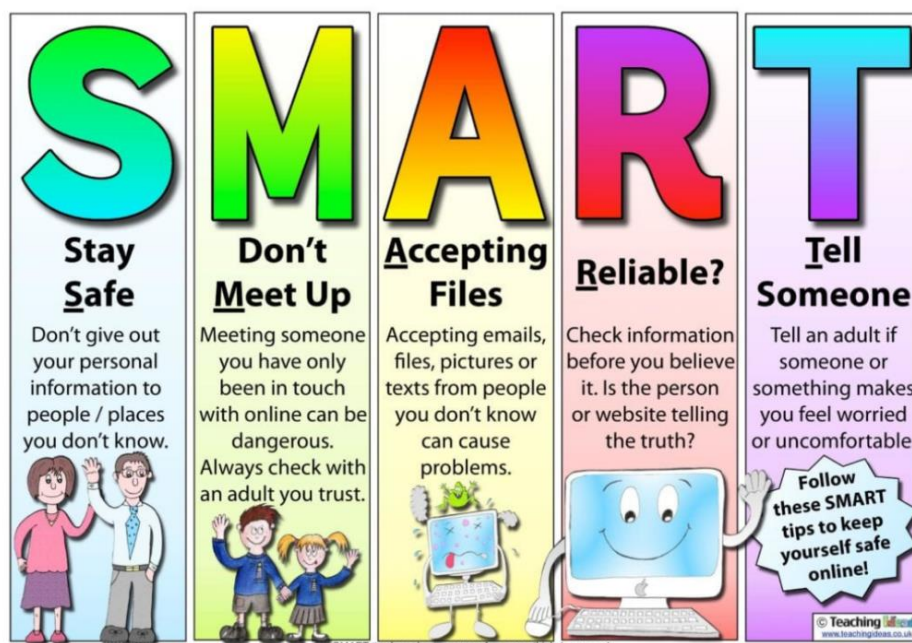
- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when emailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other students my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.

Secondary Student Acceptable Use Agreement / e-Safety Rules

These rules may need to be discussed with the pupil before they can be agreed.

I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring them into disrepute.

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc, for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to any student and will change them regularly.
- I will only use my school email address while in school.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without permission.
- I will ensure that I only use social media in school when instructed to do so by a member of staff and will follow their instructions exactly. Outside school I must not allow other social media users to know that I am a pupil at Priestley Smith School, or divulge any information which might be used by others to reveal this.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.



Staff, Governor and Visitor Acceptable Use Agreement

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign to acknowledge their receipt and understanding of this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email, Internet 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 will only use a privately owned mobile telephone in school as allowed by the school's code of conduct for such use, and never in a school motor vehicle or when carrying pupils in another vehicle.
- I will not attempt to connect any personal computer equipment (or similar) to school networks or similar systems.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not use social media on the school computers except as part of an authorised lesson or when instructed to do so by a member of school management. Outside school I must not allow other social media users to know that I am a member of Priestley Smith School staff, or divulge any information which might be used by others to assume this.
- When using social media networks or sites I am aware that I will be subject to the same standards as the school would expect for behaviour and conduct generally (as set out in the school's code of conduct). The school accepts the separation of private life and work and will not concern itself with people's private lives unless it appears that the law has been broken, or that an employee is in breach of contract, or that the school is, or will be, brought into disrepute.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils or parents.
- When conducting any school business via eMail I will only use the school e-mail system, whether in school or elsewhere.
- I will ensure that personal data (such as data held on MIS software) 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 Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will not use personal cameras, phones or similar equipment to take images of school pupils without permission. When this has been given only school media should be used to record images. Any images should be moved to the school network as soon as practicable and erased from the camera media.
- 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 without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I understand that all my use of the Internet and other related technologies is monitored and logged and can be made available, on request, to my Line Manager or 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 support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.