



Priory Junior School

Online Safety Policy

2026/27

Policy owner	Governing Board / Headteacher
Operational lead	Designated Safeguarding Lead (DSL)
Safeguarding governor	Joanne Reynolds
Last reviewed	Autumn 2026
Governing Board approval	To be confirmed
Review date	Autumn 2027
School	Priory Junior School

We LEARN with PRIDE

Peace - Respect - Independence - Determination - Equality

Contents

1. Aims
2. Legislation and guidance
3. Roles and responsibilities
4. Educating pupils about online safety
5. Educating parents/carers about online safety
6. Cyber-bullying
7. Acceptable use of the internet in school
8. Pupils using mobile devices in school
9. Staff using work devices outside school
10. How the school will respond to issues of misuse
11. Training for staff, governors and volunteers
12. Monitoring arrangements
13. Links with other policies
Appendix 1: KS2 acceptable use agreement (pupils and parents/carers)
Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)
Appendix 3: Online safety training needs - self-audit for staff
Appendix 4: Online safety incident report log

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Identify and support groups of pupils who may be at greater risk of harm online than others.
- Deliver an effective approach to online safety that empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (referred to in this policy as mobile devices).
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** - being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact** - being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes.
- **Conduct** - personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (including consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety
- Meeting digital and technology standards
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships education and health education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. It also reflects the Education Act 2011, which gives teachers powers, where there is a good reason, to search for and in exceptional circumstances delete inappropriate images or files on pupils' electronic devices in accordance with statutory guidance.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

- Make sure all staff undergo online safety training as part of child protection and safeguarding training, including their expectations, roles and responsibilities around filtering and monitoring.
- Make sure all staff receive regular online safety updates, as required and at least annually, so they continue to have the relevant skills and knowledge to safeguard children effectively.
- Co-ordinate regular discussion with appropriate staff about online safety and training needs, and monitor online safety logs provided by the DSL.
- Make sure the school teaches pupils how to keep themselves and others safe, including online.
- Make sure the school has appropriate filtering and monitoring systems on school devices and networks and regularly reviews their effectiveness. The board will review the DfE's filtering and monitoring standards and discuss with IT staff and service providers what is needed to meet them.

The filtering and monitoring standards include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions at least annually.
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
- Having effective monitoring strategies in place that meet the school's safeguarding needs.

The governor who oversees safeguarding, including online safety, is Joanne Reynolds.

All governors will:

- Make sure they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2).
- Make sure online safety is a running and interrelated theme when devising and implementing the whole-school approach to safeguarding and related policies and procedures.
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and pupils with special educational needs and/or disabilities (SEND). A one-size-fits-all approach may not be appropriate in all situations, and a more personalised or contextualised approach may be needed.

3.2 The headteacher

The headteacher is responsible for making sure that staff understand this policy and that it is implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

Details of the school's DSL and deputy DSLs are set out in the child protection and safeguarding policy and relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in making sure staff understand this policy and that it is implemented consistently.
- Working with the headteacher and governing board to review this policy annually and make sure procedures and implementation are updated regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and networks.
- Providing governors with assurance that filtering and monitoring systems are working effectively and are reviewed regularly.
- Working with the ICT manager and White Hills Park Trust IT provider to make sure appropriate systems and processes are in place.
- Working with the headteacher, ICT manager and other staff as necessary to address online safety issues or incidents.
- Managing online safety issues and incidents in line with the school's child protection and safeguarding policy.
- Responding to safeguarding concerns identified through filtering and monitoring.
- Making sure online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy.
- Making sure incidents of cyber-bullying are logged and dealt with appropriately in line with the school's behaviour policy.
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff training needs).
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or governing board.
- Undertaking annual risk assessments that consider and reflect the online risks pupils face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually.

This list is not intended to be exhaustive.

3.4 The ICT manager / IT provider

The ICT manager, working with White Hills Park Trust as the school's IT provider, is responsible for:

- Putting in place appropriate security protection procedures, including filtering and monitoring on school devices and networks, reviewed and updated at least annually to assess effectiveness and help keep pupils safe from harmful or inappropriate content and contact, including terrorist and extremist material.

- Making sure the school's ICT systems are secure and protected against viruses and malware, and that security mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Making sure online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy.
- Making sure incidents of cyber-bullying are dealt with appropriately in line with the school's behaviour policy.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy and implementing it consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and internet (appendix 2), and making sure pupils follow the school's terms on acceptable use (appendix 1).
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and knowing how to report any failure by alerting White Hills Park Trust (IT provider) and the DSL so action can be taken in line with school procedures.
- Following the correct procedure by contacting White Hills Park Trust (IT provider) if filtering and monitoring needs to be bypassed for an educational purpose.
- Working with the DSL to make sure online safety incidents are logged (appendix 4) and dealt with appropriately.
- Making sure cyber-bullying incidents are dealt with appropriately in line with the school's behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude that 'it could happen here'.

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Make sure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1).

Parents/carers can seek further guidance on keeping children safe online from organisations including the UK Safer Internet Centre and Childnet.

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to follow it. Where appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

4.1 Online safety as part of the curriculum

This section reflects the National Curriculum computing programmes of study and the government's relationships education and health education guidance for introduction from 1 September 2026.

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.
- Be discerning in evaluating digital content.

By the end of primary school, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. This includes avoiding putting pressure on others to share information or images online and using strategies to resist peer pressure.

- How to critically evaluate online relationships and sources of information, including risks associated with people they have never met. This includes understanding that people may pretend to be someone else, including pretending to be a child, recognising harmful content or contact and knowing how to report it.
- That there is a minimum age for joining social media sites (currently 13), which is intended to protect children from inappropriate content and unsafe contact with older users, who may be strangers, including other children and adults.
- The importance of exercising caution about sharing information about themselves online and using privacy and location settings to protect information.
- That material provided online may be circulated, and that once a picture or words have been circulated it may not be possible to delete them everywhere or control where they end up.
- That the internet contains content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and pupils with SEND.

4.2 Practical cyber security skills

The following areas reflect the DfE's non-statutory cyber security standards for schools and colleges.

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information.
- Password security.
- Social engineering.
- The risks of removable storage devices (for example USB drives).
- Multi-factor authentication.
- How to report a cyber incident or attack.
- How to report a personal data breach.

Pupils will also receive age-appropriate education on safeguarding issues such as cyber-bullying and the risks of online radicalisation.

5. Educating parents/carers about online safety

The school will raise parents'/carers' awareness of online safety through letters or other communications home and information on the school website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school, if anyone, their child will be interacting with online.

Queries or concerns about online safety should be raised in the first instance with the headteacher and/or DSL. Concerns or queries about this policy may be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. See also the school's behaviour policy.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will make sure pupils understand what it is and what to do if they become aware of it happening to them or others. Pupils will know how to report incidents and will be encouraged to report concerns, including where they are a witness rather than the target.

The school will actively discuss cyber-bullying with pupils, explaining why it occurs, the forms it may take and the possible consequences. Class teachers will discuss cyber-bullying with their classes.

Teaching staff will use opportunities across the curriculum to cover cyber-bullying, including relationships, social, health and economic (RSHE) education and other subjects where appropriate.

All staff, governors and volunteers, where appropriate, will receive training on cyber-bullying, its impact and ways to support pupils as part of safeguarding training.

The school will also provide information to parents/carers so they are aware of the signs, how to report cyber-bullying and how they can support children who may be affected.

For a specific incident, the school will follow the processes in its behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to contain the incident.

The DSL will report the incident and provide relevant material to the police as soon as reasonably practicable where there are reasonable grounds to suspect that possessing the material is illegal. The DSL will also work with external services where necessary.

6.3 Examining electronic devices

The headteacher, and any member of staff specifically authorised to do so by the headteacher in line with the school's behaviour policy, may carry out a search and confiscate an electronic device where there are reasonable grounds for suspecting that it:

- Poses a risk to staff or pupils; and/or
- Is identified in school rules as a banned item for which a search can be carried out; and/or
- Is evidence in relation to an offence.

Before a search, the authorised staff member will:

- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, advice will be sought from the headteacher, DSL or another appropriate senior member of staff.
- Explain to the pupil why they are being searched and how the search will happen, and give them an opportunity to ask questions.
- Seek the pupil's co-operation.

Authorised staff may examine, and in exceptional circumstances erase, data or files on a confiscated electronic device where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine data or files, the staff member should reasonably suspect that the device has been, or could be, used to:

- Cause harm; and/or
- Undermine the safe environment of the school or disrupt teaching; and/or
- Commit an offence.

If inappropriate material is found, the authorised staff member will decide on a suitable response in conjunction with the DSL, headteacher or another member of the senior leadership team. If images, data or files may put a person at risk, the safeguarding response will be considered first.

When deciding whether there is a good reason to erase data or files, staff will consider whether the material may be evidence relating to a suspected offence. If it may be evidence, it will not be deleted and the device will be handed to the police as soon as reasonably practicable. If it is not suspected to be evidence of an offence, staff may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person; and/or
- The pupil and/or parent/carer refuses to delete the material themselves.

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image.
- Confiscate the device and report the incident to the DSL immediately. The DSL will decide what to do next in line with the latest DfE guidance on searching, screening and confiscation and UKCIS guidance on sharing nudes and semi-nudes.

Any searching of pupils will be carried out in line with the latest DfE guidance on searching, screening and confiscation, UKCIS guidance on sharing nudes and semi-nudes, and the school's behaviour policy.

Any complaint about searching for or deleting inappropriate images or files on a pupil's electronic device will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative AI tools are widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Priory Junior School recognises that AI can support learning, but may also be used to bully or harm others. This includes 'deepfakes', where AI is used to create images, audio or video that appear real, including deepfake pornography created using a person's likeness.

Priory Junior School will treat any use of AI to bully pupils very seriously, in line with the school's behaviour policy.

Staff should be aware of the risks of AI tools while they are developing and should carry out a risk assessment where new AI tools are introduced by the school, or where existing AI tools are used in ways that may pose a risk to individuals, including pupils and staff.

Where the school or trust adopts a separate AI usage policy, this policy should be read alongside it.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding acceptable use of the school's ICT systems and internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use where relevant.

Use of the school's internet must be for educational purposes only, or for fulfilling the duties of an individual's role.

The school will monitor websites visited by pupils, staff, volunteers, governors and visitors, where relevant, and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but they are not permitted to use them during:

- School hours.
- Clubs before or after school, or any other activities organised by the school, unless a member of staff has given specific permission.

Any permitted use of a mobile device in school must be in line with the pupil acceptable use agreement (appendix 1).

A breach of the acceptable use agreement may trigger action in line with the school's behaviour policy and may result in confiscation of the device.

9. Staff using work devices outside school

All staff members will take appropriate steps to keep work devices secure, including:

- Keeping the device password-protected. Strong passwords may use three random words, combined with numbers and special characters where required, or be generated by a password manager.
- Ensuring the hard drive is encrypted so files cannot be accessed by attaching a lost or stolen drive to another device.
- Making sure the device locks after a period of inactivity.
- Not sharing the device with family or friends.
- Using appropriate anti-virus and anti-spyware protection.
- Keeping operating systems up to date by installing updates promptly.

Staff must not use a work device in a way that would breach the school's acceptable use terms (appendix 2).

Work devices must be used solely for work activities.

If staff have concerns about the security of a device, they must seek advice from the headteacher, a member of the senior leadership team or the ICT/IT provider as appropriate.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, the school will follow its behaviour and ICT/internet acceptable use procedures. Action will depend on the circumstances, nature and seriousness of the incident and will be proportionate.

Where a staff member misuses the school's ICT systems or internet, or misuses a personal device in a way that constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct and/or disciplinary procedures. Action will depend on the individual circumstances, nature and seriousness of the incident.

The school will consider whether incidents involving illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training for staff, governors and volunteers

All new staff members will receive training as part of induction on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required, for example through emails, e-bulletins and staff meetings.

Through this training, staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and children are at risk of online abuse.
- Children can abuse their peers online through abusive, threatening, harassing or misogynistic messages; non-consensual sharing of indecent nude or semi-nude images and/or videos; and sharing abusive images or pornography with those who do not want to receive such content.
- Physical abuse, sexual violence and initiation/hazing-type violence can all contain an online element.

Training will also help staff to:

- Develop better awareness to help spot the signs and symptoms of online abuse.
- Help pupils recognise dangers and risks in online activity and weigh up those risks.
- Influence pupils to make healthy long-term choices and keep themselves safe from harm in the short term.

The DSL and deputy DSLs will undertake child protection and safeguarding training, including online safety, at least every two years. They will update their knowledge and skills on online safety at regular intervals and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of safeguarding training. Volunteers will receive appropriate training and updates where applicable.

More information about safeguarding training is set out in the child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. The online safety incident report log is included at appendix 4.

This policy will be reviewed every year by the headteacher, or a person delegated by the headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the online risks pupils face, recognising that technology and related risks and harms evolve rapidly.

13. Links with other policies

This online safety policy is linked to the school's:

- Child protection and safeguarding policy.
- Behaviour policy.
- Staff code of conduct and disciplinary procedures.
- Data protection policy and privacy notices.
- Complaints procedure.
- ICT and internet acceptable use policy.

Appendix 1: KS2 acceptable use agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET - AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil: _____

I will read and follow the rules in this acceptable use agreement.

When I use the school's ICT systems and internet in school I will:

- Use the school's ICT systems and internet responsibly and for educational purposes only.
- Only use them when a teacher is present or with a teacher's permission.
- Keep my usernames and passwords safe and not share them with others.
- Keep my private information safe and not give my name, address, telephone number, location or other personal information to anyone without the permission of my teacher or parent/carer.
- Tell a teacher or another trusted adult immediately if I find material that might upset, distress or harm me or others.
- Always log off or shut down a computer when I have finished using it.

I will not:

- Access inappropriate websites, including social networking sites, chat rooms and gaming sites, unless a teacher has expressly allowed this as part of a learning activity.
- Open email attachments or follow links in emails without first checking with a teacher.
- Use inappropriate language when communicating online, including in emails or messaging.
- Create, link to, post or share material that is pornographic, offensive, obscene or otherwise inappropriate.
- Log in to the school network using someone else's details.
- Arrange to meet anyone offline without first consulting my parent/carer and without appropriate adult supervision.

If I bring a personal mobile phone, smart watch or other personal electronic device into school:

- I will not use it during school hours, clubs or other activities organised by the school unless a teacher gives me permission.
- I will use it responsibly and will not access inappropriate material or use inappropriate language when communicating online.

I understand that the school monitors use of its systems and internet and that there will be consequences if I do not follow these rules.

Signed (pupil): _____ Date: _____

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of staff. I agree to the conditions above and will make sure my child understands them.

Signed (parent/carer): _____ Date: _____

Appendix 2: Acceptable use agreement for staff, governors, volunteers and visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET

Name: _____

When using the school's ICT systems and accessing the internet in school, or outside school on a work device where applicable, I will not:

- Access or attempt to access inappropriate material, including material of a violent, criminal or pornographic nature, or create, share, link to or send such material.
- Use the systems in any way that could harm the school's reputation.
- Access social networking sites or chat rooms except where specifically authorised for a legitimate work purpose.
- Use improper language when communicating online, including in email or other messaging services.
- Install unauthorised software or connect unauthorised hardware or devices to the school network.
- Share my password with others or log in using another person's credentials.
- Take photographs of pupils without following school procedures and checking that this is authorised.
- Share confidential information about the school, its pupils or staff, or other members of the community.
- Access, modify or share data I am not authorised to access, modify or share.
- Promote private businesses unless directly related to an authorised school activity.

I will only use the school's ICT systems and internet for educational purposes or to fulfil the duties of my role.

I understand that the school monitors use of its ICT facilities and systems in accordance with safeguarding, security and data protection requirements.

I will take reasonable steps to keep work devices secure and password-protected outside school and will keep data securely stored in line with this policy and the school's data protection policy.

I will inform the DSL and ICT manager/IT provider if a pupil tells me they have found material that may upset, distress or harm them or others, and I will do the same if I encounter such material.

I will use the school's ICT systems and internet responsibly and will make sure pupils in my care do so too.

Signed: _____ Date: _____

Appendix 3: Online safety training needs - self-audit for staff

Name of staff member/volunteer: _____ Date: _____

Question	Yes/No	Comments
Do you know the name of the person who has lead responsibility for online safety in school?		
Are you aware of the ways pupils can abuse their peers online?		
Do you know what you must do if a pupil approaches you with an online safety concern or issue?		
Are you familiar with the school's acceptable use agreement for staff, governors, volunteers and visitors?		
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?		
Are you familiar with the filtering and monitoring systems on the school's devices and networks?		
Do you understand your role and responsibilities in relation to filtering and monitoring?		
Do you follow the school's password and account security requirements?		
Are you familiar with the school's approach to tackling cyber-bullying?		
Do you understand the school's expectations and risk-assessment approach for AI tools?		
Are there any areas of online safety in which you would like training or further training?		

Appendix 4: Online safety incident report log

Use this log to record online safety incidents and actions taken. Safeguarding concerns must also be recorded and managed through the school's safeguarding procedures.

Date	Where incident took place	Description of incident	Action taken	Name/signature of staff member