POLICY DOCUMENT

Online Safety Policy

Princess May Primary School's approach to online safety — 2026–2027

Governing Body Representative (GBR)	Kristofer McGhee (Chair of Governors)
Signed by (GBR)	……
Date approved	4 September 2026
Next review due by	September 2027
Related policies	Safeguarding and Child Protection Policy; Behaviour Policy; Anti-Bullying Policy; Mobile Phone Policy; Prevent Duty Policy; Data Protection Policy
Aligned to	Keeping Children Safe in Education 2026 (in force from 1 September 2026); the DfE's guidance on Teaching Online Safety in Schools, Preventing and Tackling Bullying, Relationships Education, Relationships and Sex Education (RSE) and Health Education, and Searching, Screening and Confiscation; the DfE's statutory guidance, Mobile Phones in Schools (June 2026 edition); the DfE's guidance on Generative Artificial Intelligence in Education; the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Equality Act 2010 and the Education Act 2011; and the National Curriculum computing programmes of study

1. Aims

Our school aims to:

- have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology; and
- 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, disinformation, misinformation and 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 them 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 the consensual and non-consensual sharing of nudes and semi-nudes, which now includes AI-generated or digitally altered images such as deepfakes, sharing other explicit images, and online bullying; and
- commerce — risks such as online gambling, inappropriate advertising, phishing and financial scams.

2. Legislation and guidance

This policy is based on the DfE's statutory safeguarding guidance, Keeping Children Safe in Education 2026 (in force from 1 September 2026), and its advice for schools on Teaching Online Safety in Schools, Preventing and Tackling Bullying, Relationships Education, Relationships and Sex Education (RSE) and Health Education, and Searching, Screening and Confiscation. It also refers to the DfE's guidance on protecting children from radicalisation, and its statutory guidance, Mobile Phones in Schools (June 2026 edition, in force from 1 September 2026), which requires us to be a mobile phone-free environment by default; see our Mobile Phone Policy for more detail.

KCSIE 2026 has updated its online risk categories to reflect the increasing presence of artificial intelligence, and now requires schools to review the effectiveness of their filtering and monitoring systems at least once every academic year. We also have regard to the DfE's guidance on Generative Artificial Intelligence in Education when considering how pupils and staff use AI tools safely.

This policy also has regard to the DfE's non-statutory guidance, Preventing and Tackling Bullying and Harassment of School Staff (July 2026), which replaced the previous 2014 advice for headteachers and school staff and includes updated online safety guidance for staff who experience bullying or harassment online.

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 stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on a pupil's electronic device where they believe there is a good reason to do so. The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

The governing body

The governing body has overall responsibility for monitoring this policy, and holding the Headteacher to account for its implementation. The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs provided by the DSL. All governors will:

- ensure they have read and understood this policy;
- agree and adhere to the terms on acceptable use of the school's ICT systems and the internet, at Appendix 3;
- ensure that online safety is a running, interrelated theme when devising and implementing the school's wider approach to safeguarding and related policies and procedures; and
- ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse, and some pupils with special educational needs and/or disabilities, recognising that a one-size-fits-all approach may not suit every child.

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of our DSL and Deputy DSLs are set out in our Safeguarding and Child Protection Policy and relevant job descriptions. The DSL takes lead responsibility for online safety, in particular:

- supporting the Headteacher in ensuring staff understand this policy, and that it is implemented consistently;
- working with the Headteacher, ICT support technician and other staff, as necessary, to address any online safety issue or incident;
- managing all online safety issues and incidents in line with our Safeguarding and Child Protection Policy;
- ensuring any online safety incident is logged and dealt with appropriately in line with this policy;
- ensuring any incident of cyber-bullying is logged and dealt with appropriately in line with our Behaviour Policy;
- updating and delivering staff training on online safety;
- liaising with other agencies or external services if necessary; and
- providing regular reports on online safety to the Headteacher and/or governing board.

This list is not intended to be exhaustive.

The ICT support technician

The ICT support technician, currently provided by Badger Computer Services Ltd, is responsible for:

- putting in place an appropriate level of security protection, such as filtering and monitoring systems, reviewed and updated regularly to assess their effectiveness, at least once every academic year, and to ensure pupils are kept safe from potentially harmful and inappropriate content and contact online, including terrorist and extremist material;
- ensuring the school's ICT systems are secure and protected against viruses and malware, with safety mechanisms updated regularly;
- conducting a full security check and monitoring the school's ICT systems on a weekly basis;
- blocking access to potentially dangerous sites, and, where possible, preventing the downloading of potentially dangerous files;

- ensuring any online safety incident is logged and dealt with appropriately in line with this policy; and
- ensuring any incident of cyber-bullying is dealt with appropriately in line with our Behaviour Policy.

This list is not intended to be exhaustive.

All staff and volunteers

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

- maintaining an understanding of this policy;
- implementing this policy consistently;
- agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, at Appendix 3, and ensuring pupils follow the school's terms on acceptable use, at Appendices 1 and 2;
- working with the DSL to ensure any online safety incident is logged and dealt with appropriately in line with this policy;
- ensuring any incident of cyber-bullying is dealt with appropriately in line with our Behaviour Policy; and
- responding appropriately to all reports and concerns about sexual violence and/or harassment, online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- notify a member of staff or the Headteacher of any concern or query about this policy; and
- ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet, at Appendices 1 and 2.

Parents can seek further guidance on keeping children safe online from the UK Safer Internet Centre, Childnet International, and CEOP's Thinkuknow website.

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, when relevant, and expected to read and follow it; if appropriate, they will be expected to agree to the terms on acceptable use at Appendix 3.

4. Educating pupils about online safety

Pupils are taught about online safety as part of the curriculum. All schools must teach Relationships Education and Health Education, in line with the DfE's statutory guidance, updated for 2026.

In Early Years Foundation Stage and Key Stage 1, pupils are taught to:

- use technology safely and respectfully, keeping personal information private; and
- identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Key Stage 2 are taught to:

- use technology safely, respectfully and responsibly;
- recognise acceptable and unacceptable behaviour; and
- identify a range of ways to report concerns about content and contact.

By the end of primary school, pupils will know:

- that people sometimes behave differently online, including by pretending to be someone they are not;
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous;
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them;
- how to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met;
- how information and data is shared and used online;
- what sorts of boundaries are appropriate in friendships with peers and others, including in a digital context; and
- how to respond safely and appropriately to adults they may encounter, in any context including online, whom they do not know.

The safe use of social media and the internet is also covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse, and some pupils with SEND, with specific and tailored guidance provided to individual children, groups and/or parents and carers as appropriate, including in response to a specific online safety incident.

5. Educating parents about online safety

The school raises parents' awareness of internet safety through letters and other communications home, and through information on our website and in our newsletter; this policy is also shared with parents, and online safety is covered during parent consultations.

The school will let parents know what systems it uses to filter and monitor online use, and 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.

If parents have any query or concern about online safety, this should be raised in the first instance with the Headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Cyber-bullying

Definition

Cyber-bullying takes place online, for example 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, where the relationship involves an imbalance of power; see also our Anti-Bullying Policy.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we ensure pupils understand what it is and what to do if they become aware of it happening to them or others, including where they are a witness rather than the person targeted, and we encourage pupils to report any incident.

The school actively discusses cyber-bullying with pupils, explaining why it occurs, the forms it may take, and its consequences. Teaching staff deliver sessions from the Kapow Computing and PSHE/RSE schemes of work to cover cyber-bullying, and all staff receive training on cyber-bullying, its impact, and ways to support pupils, as part of safeguarding training — see Section 11 for more detail. The school also sends information and leaflets on cyber-bullying to parents, so they are aware of the signs, how to report it, and how to support a child who may be affected.

In relation to a specific incident of cyber-bullying, the school follows the processes set out in our Behaviour Policy and Anti-Bullying Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal, and will work with external services where necessary. Cyber-bullying incidents are recorded on CPOMS.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement on the acceptable use of the school's ICT systems and the internet, at Appendices 1 to 3; visitors are expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or to fulfil the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors, where relevant, to ensure they comply with this; more information is set out in the acceptable use agreements at Appendices 1 to 3.

8. Pupils using mobile devices in school

In line with our Mobile Phone Policy, Princess May is a mobile phone-free environment by default: pupils are not expected to bring a mobile phone to school. Where a parent or carer feels this is necessary — for example, because their child travels to or from school independently — permission must be agreed in advance with the school office, using the permission form in our Mobile Phone Policy.

Where a phone is brought in with permission, it must be handed to the class teacher at the start of the day, switched off; the class teacher will lock it away securely for the day, and return it at the end of the day; it is not accessed at any point during the school day. Pupils attending an after-school club collect their phone from the class teacher at the end of the school day and hand it to the club leader, who returns it when the child is collected.

The school accepts no responsibility for the loss of, or damage to, a phone while it is stored on site.

9. Staff using work devices outside school

All staff will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- keeping the device password-protected;
- making sure the device locks if left inactive for a period of time;
- not sharing the device with family or friends; and
- keeping operating systems up to date, by always installing the latest updates.

Staff must not use a work device in any way that would violate the school's terms of acceptable use, set out at Appendix 3, and a work device must be used solely for work activities. If staff have any concern about the security of their device, they should seek advice from the school's ICT support service provider.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour Policy; the action taken will depend on the individual circumstances, nature and seriousness of the incident, and will be proportionate. The incident will be recorded on CPOMS.

Where a staff member misuses the school's ICT systems or internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with staff disciplinary procedures; the action taken will depend on the individual circumstances, nature and seriousness of the incident. The school will consider whether an incident involving illegal activity or content, or another otherwise serious incident, should be reported to the police.

11. Training

Staff receive training on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation. All staff 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 or staff meetings.

Through this training, all staff are 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, harassing or misogynistic messages, the non-consensual sharing of indecent nude or semi-nude images or videos, including in chat groups, and the sharing of abusive images or pornography with those who don't want to receive it; and
- physical abuse, sexual violence and initiation or hazing-type violence can all contain an online element.

Training also helps staff develop a better awareness to spot the signs and symptoms of online abuse, to help pupils recognise dangers and risks in online activity and weigh these up, and to help pupils make the healthiest long-term choices while keeping them safe from short-term harm.

The DSL and Deputy DSLs undertake child protection and safeguarding training, including online safety, at least every 2 years, and update their knowledge and skills on online safety at regular intervals, and at least annually. Governors receive training on safe internet use and online safeguarding as part of their safeguarding training, and volunteers receive appropriate training and updates where applicable. More information is set out in our Safeguarding and Child Protection Policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS. This policy will be reviewed every year by the Online Safety lead, DSL and/or Deputy DSLs; at every review, the policy will be shared with the governing board. The review is supported by an annual risk assessment considering the risks pupils face online, since technology, and the risks and harms associated with it, continue to evolve and change rapidly.

13. Links to other policies

- Safeguarding and Child Protection Policy;
- Behaviour Policy;
- Anti-Bullying Policy;
- Mobile Phone Policy;
- staff disciplinary procedures; and
- Data Protection Policy and privacy notices.

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

When I use the school's ICT systems, like computers, and get onto the internet in school, I will:

- ask a teacher or adult if I can do so before using them;
- only use websites that a teacher or adult has told me or allowed me to use;
- tell my teacher immediately if I click on a website by mistake, receive a message from someone I don't know, or find anything that may upset or harm me or my friends;
- use school computers for school work only;
- be kind to others, and not upset or be rude to them;
- look after the school's ICT equipment, and tell a teacher straight away if something is broken or not working properly;
- only use the username and password I have been given, and try my hardest to remember them;
- never share my password with anyone, including my friends;
- never give my personal information — my name, address or telephone number — to anyone without the permission of my teacher or parent/carer;
- save my work on the school network;
- check with my teacher before I print anything; and
- log off or shut down a computer when I have finished using it.

I agree that the school will monitor the websites I visit, and that there will be consequences if I don't follow the rules.

Signed (pupil): ..... Date: .....

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

Signed (parent/carer): ..... Date: .....

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

I will read and follow the rules in this acceptable use agreement. When I use the school's ICT systems, like computers, and get onto the internet in school, I will:

- always use the school's ICT systems and the 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 these with others;
- keep my private information safe at all times, and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer;
- tell a teacher, or another sensible adult, immediately if I find any material which might upset, distress or harm me or others; and
- always log off or shut down a computer when I've finished working on it.

I will not:

- access any inappropriate website, including social networking sites, chat rooms and gaming sites, unless my teacher has expressly allowed this as part of a learning activity;
- open any attachment in an email, or follow any link in an email, without first checking with a teacher;
- use any inappropriate language when communicating online, including in emails;
- create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate;
- log in to the school's network using someone else's details; or
- arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.

If I bring a mobile phone to school, I will hand it to my class teacher at the start of the day and collect it at the end of the day.

If I bring any other personal electronic device into school:

- I will use it responsibly, and will not access any inappropriate website or other inappropriate material, or use inappropriate language when communicating online.

I agree that the school will monitor the websites I visit, and that there will be consequences if I don't follow the rules.

Signed (pupil): ..... Date: .....

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer): ..... Date: .....

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

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 but not limited to material of a violent, criminal or pornographic nature, or create, share, link to or send such material;
- use them in any way that could harm the school's reputation;
- access social networking sites or chat rooms;
- use any improper language when communicating online, including in emails or other messaging services;
- install any unauthorised software, or connect any unauthorised hardware or device to the school's network;
- share my password with others, or log in to the school's network using someone else's details;
- take a photograph of a pupil without checking with teachers first;
- share confidential information about the school, its pupils or staff, or another member of the community;
- access, modify or share data I am not authorised to access, modify or share; or
- promote a private business, unless that business is directly related to the school.

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or to fulfil the duties of my role. I agree that the school will monitor the websites I visit, and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that a work device is secure and password-protected when I use it outside school, and keep all data securely stored in line with this policy and the school's Data Protection Policy.

I will let the DSL and ICT support technician know if a pupil tells me they have found material which might upset, distress or harm them or others, and will also do so if I encounter such material myself. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor): .....
Date: .....