Primary School Online Safety and Safeguarding Policy (2026)

A guide for schools on what to include in their online safety policies to meet RSHE 2025 and KCSIE 2025 requirements.

Introduction

Online safety is now a core part of keeping children safe in school. This document sets out what primary schools in England need to include in their online safety policies from 2026, based on the latest statutory guidance: RSHE 2025 and Keeping Children Safe in Education (KCSIE) 2025.

Schools must have clear policies that cover what children are taught (RSHE curriculum) and how adults keep them safe (safeguarding systems, filtering, monitoring, staff training).

Part 1: What is an Online Safety Policy?

An online safety policy is a document that explains:

- What children will learn about staying safe online (RSHE content)
- How the school filters and monitors devices and the internet
- What staff and pupils are expected to do online (acceptable use)
- How the school responds if something goes wrong (reporting and support)
- How parents and carers are involved

It is a legal requirement under KCSIE 2025 and should be shared with all staff, parents and governors.

Part 2: Online Safety Curriculum (What Children Learn)

Primary KS1 (Ages 5–7)

Children learn simple rules for staying safe:

- **Device use**: How to use devices kindly and ask a grown-up before downloading apps or clicking links.
- **Personal information**: What information is private (name, home address, school name, photos) and when it's OK to share.

- **Being kind online**: How to be kind in messages; not sending mean, rude or scary messages.
- **Telling a trusted adult**: When something feels wrong or uncomfortable online, tell a teacher or parent
- **Spotting tricks**: Pop-ups, ads and "too good to be true" offers are not real and you should tell an adult

Primary KS2 (Ages 7–11)

Children learn more critical thinking and can start to understand online risks:

- **Online friendships**: How online friendships can be real or fake; how to stay safe when chatting to people you don't know; not sharing secrets online
- **Gaming safety**: Loot boxes, in-game spending, age ratings, why some games cost real money and scams involving free Robux or V-Bucks
- **Image and photo safety**: Never sharing photos of yourself or others without permission; understanding that once something is online, it can spread; early age-appropriate discussion of pressure to share images (upper KS2 only, with sensitivity)
- **Data and privacy**: How apps and websites collect information about you; location settings; why passwords matter
- **Media literacy**: How to spot fake news, misleading adverts, fake accounts and AI-generated images; not believing everything online
- **Online wellbeing**: How spending lots of time online can affect sleep, mood, friendships and feeling good about yourself
- **Financial online harms**: Scams, phishing emails ("You've won..."), fake competitions and why you need a grown-up to spend money online

Part 3: Filtering, Monitoring and Tech Safety

Schools must show they have systems in place to keep children safe online. This section of your policy should cover:

Filtering and Blocking

- The school uses filtering software to block harmful, age-inappropriate and illegal content (violent, sexual, hateful material)
- Filtering is reviewed at least once a year to check it is working and not over-blocking learning
- A named person (usually the DSL or IT lead) is responsible for checking and updating filters

Monitoring and Logging

- The school monitors school devices and networks to watch for concerning behaviour (bullying, contact with unknown adults, accessing blocked sites)
- Staff know how to log and report concerns if a child is acting unsafely online
- Records of monitoring are kept and reviewed regularly.

Acceptable Use Policies (AUPs)

- Pupils, staff and parents have signed an acceptable use agreement that explains what you can and cannot do on school devices and the school network
- AUPs include rules about:
  - Not sending unkind, rude or threatening messages
  - Not sharing other people's photos or personal details
  - Not downloading apps or visiting websites without permission
  - Not using school devices for illegal activity (plagiarism, cyberbullying, viewing harmful material)

Generative AI and New Tools

- The school has clear guidance on when and how pupils can use AI tools (e.g. ChatGPT, image generators) in lessons
- Staff and pupils understand that AI-generated content can be misleading or inaccurate and that data shared with AI tools is tracked
- AI tools are not used by very young children without careful supervision and consent

Part 4: Roles and Responsibilities

Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- Overseeing the school's online safety policy and checking it is working
- Making sure filtering and monitoring systems are in place and reviewed annually
- Training staff on online safety and current risks (AI, misinformation, gaming harms)
- Handling reports of online incidents (bullying, grooming, contact with unknown adults) and involving parents and police if needed
- Working with governors to make sure online safety is part of the whole-school safeguarding approach

All Staff

- Know the online safety policy and can spot signs a child may be experiencing harm online
- Know how to report concerns to the DSL
- Model safe, respectful online behaviour themselves

- Teach online safety as part of RSHE, computing and across the curriculum

Governors

- Make sure the school has an online safety policy and that it is reviewed at least annually
- Check that filtering, monitoring and staff training are in place
- Hear about online safety incidents and trends so they can support the school's approach

Parents and Carers

- Are given clear information about what the school teaches about online safety
- Are involved in safeguarding decisions if their child has experienced online harm
- Receive regular newsletters, workshops or webinars about how they can keep their child safe at home

Part 5: What to Do if Something Goes Wrong

Reporting Online Incidents

If a child or staff member spots something concerning online (bullying, contact with unknown adults, harmful content, sexual images), they should:

- Tell a trusted adult (teacher, office staff, DSL) immediately
- Save evidence (screenshots, dates, times, usernames) if safe to do so
- Not delete the content (it may be needed for investigation)

School's Response

The school will:

- Listen to the child and take concerns seriously
- Assess the level of harm and involve parents/carers
- Follow the school's safeguarding procedures (child protection plan, early help if needed)
- Involve police if the content is illegal (sexual images of children, extreme violence, threats)
- Support the child and any other children involved
- Record the incident and review lessons learned

Support for Children

- The school provides counselling, emotional support or mentoring to help children recover
- The school teaches about resilience, reporting and staying safe in follow-up RSHE lessons
- Parents are kept informed and given advice on how to support at home

Part 6: Working with Parents and Families

Schools must actively involve families in online safety, as expected by KCSIE 2025 and RSHE guidance. This means:

Sharing Information

- Online safety policy is published on the school website and shared in paper copies on request
- Termly or half-termly newsletters explain online safety topics being taught (e.g. "This term we're learning about loot boxes and gaming")
- School website has a dedicated page with resources and tips for parents on online safety

Parent Workshops and Webinars

- Annual or termly parent sessions on topics like:
  - Gaming safety and loot boxes
  - Social media and misogynistic influencers
  - Scams and financial online harms
  - AI and deepfakes: what they are and why they matter
  - How to talk to your child about online safety

Home-School Agreement

- Parents are asked to sign a home-school agreement that includes a commitment to support online safety (e.g. monitoring their child's device use, knowing what apps their child uses, talking about online risks)

Part 7: Annual Review and Updates

The online safety policy must be reviewed at least once a year (usually in summer term) to:

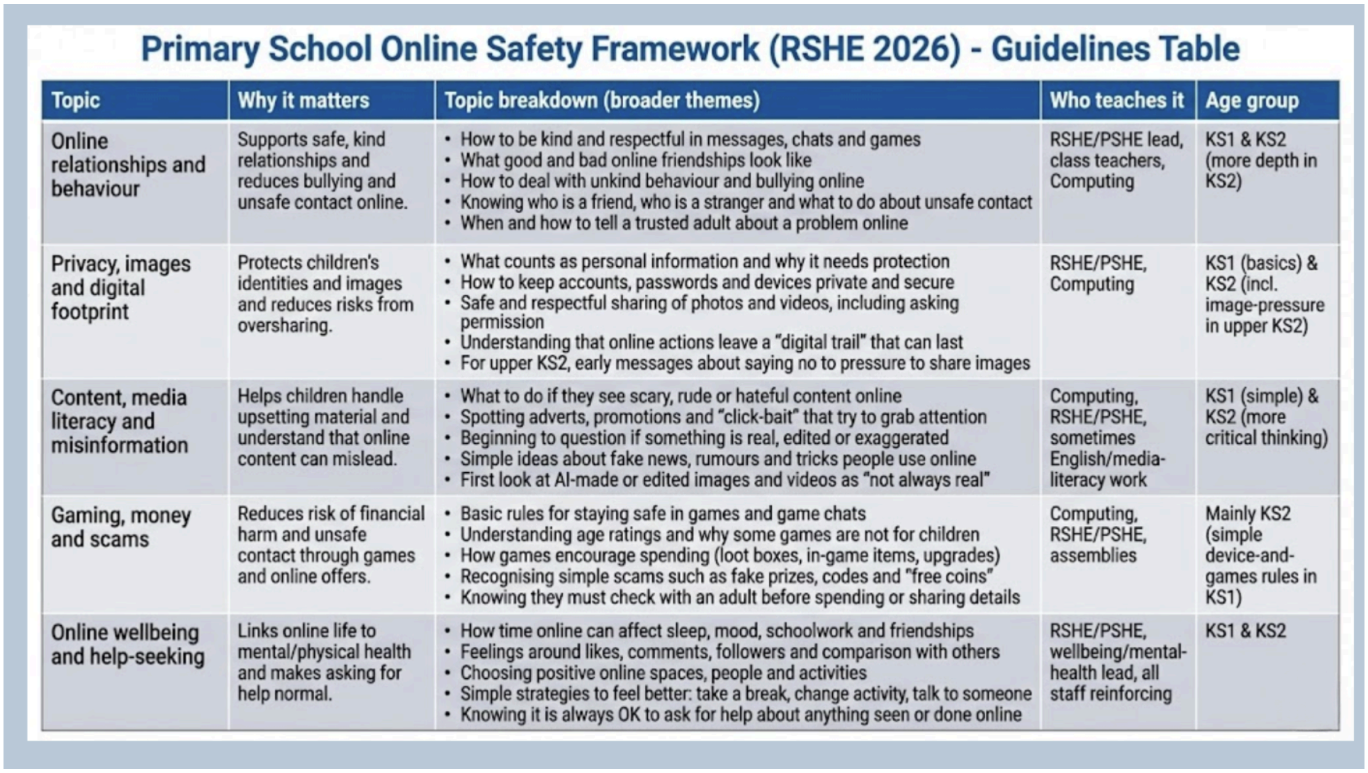
- Check it still reflects current online risks and harms (e.g. new apps, AI, changes in how children are using the internet)
- Make sure filtering and monitoring systems are working
- Include feedback from staff, pupils, parents and governors

- Update RSHE content if new statutory guidance is released
- Reflect any new tools or platforms the school is using (e.g. new learning platforms, AI in lessons)

Part 8: Key Online Safety Topics for 2026

Based on RSHE 2025 and KCSIE 2025, schools should ensure their policy and curriculum

Table 1: Key Online Safety Topics for 2026 Curriculum



Primary School Online Safety Framework (RSHE 2026) - Guidelines Table

Topic	Why it matters	Topic breakdown (broader themes)	Who teaches it	Age group
Online relationships and behaviour	Supports safe, kind relationships and reduces bullying and unsafe contact online.	• How to be kind and respectful in messages, chats and games • What good and bad online friendships look like • How to deal with unkind behaviour and bullying online • Knowing who is a friend, who is a stranger and what to do about unsafe contact • When and how to tell a trusted adult about a problem online	RSHE/PSHE lead, class teachers, Computing	KS1 & KS2 (more depth in KS2)
Privacy, images and digital footprint	Protects children's identities and images and reduces risks from oversharing.	• What counts as personal information and why it needs protection • How to keep accounts, passwords and devices private and secure • Safe and respectful sharing of photos and videos, including asking permission • Understanding that online actions leave a "digital trail" that can last • For upper KS2, early messages about saying no to pressure to share images	RSHE/PSHE, Computing	KS1 (basics) & KS2 (incl. image-pressure in upper KS2)
Content, media literacy and misinformation	Helps children handle upsetting material and understand that online content can mislead.	• What to do if they see scary, rude or hateful content online • Spotting adverts, promotions and "click-bait" that try to grab attention • Beginning to question if something is real, edited or exaggerated • Simple ideas about fake news, rumours and tricks people use online • First look at AI-made or edited images and videos as "not always real"	Computing, RSHE/PSHE, sometimes English/media-literacy work	KS1 (simple) & KS2 (more critical thinking)
Gaming, money and scams	Reduces risk of financial harm and unsafe contact through games and online offers.	• Basic rules for staying safe in games and game chats • Understanding age ratings and why some games are not for children • How games encourage spending (loot boxes, in-game items, upgrades) • Recognising simple scams such as fake prizes, codes and "free coins" • Knowing they must check with an adult before spending or sharing details	Computing, RSHE/PSHE, assemblies	Mainly KS2 (simple device-and-games rules in KS1)
Online wellbeing and help-seeking	Links online life to mental/physical health and makes asking for help normal.	• How time online can affect sleep, mood, schoolwork and friendships • Feelings around likes, comments, followers and comparison with others • Choosing positive online spaces, people and activities • Simple strategies to feel better: take a break, change activity, talk to someone • Knowing it is always OK to ask for help about anything seen or done online	RSHE/PSHE, wellbeing/mental-health lead, all staff reinforcing	KS1 & KS2

Part 9: What Inspectors (Ofsted) Look For

Ofsted inspectors will check that your school's online safety approach includes:

- A clear, up-to-date online safety policy that staff know and follow
- Evidence that filtering and monitoring are in place and regularly reviewed
- Teaching about online safety across RSHE, computing and the wider curriculum
- Staff training on current online risks and how to respond to concerns
- A culture where children feel safe to report online problems
- Parent engagement and involvement in online safety

- A record of online incidents and how they were handled

Appendix: Quick Checklist for Primary Schools

Does your online safety policy include:

- Clear curriculum content for KS1 and KS2 on all topics in Part 8?
- Details of your filtering and monitoring systems and annual review cycle?
- Roles and responsibilities for DSL, staff, governors and parents?
- Clear reporting and response procedures for online incidents?
- Information about parent workshops, newsletters and home-school agreements?
- A named responsible person for online safety and DSL oversight?
- Specific guidance on AI tools, generative content and new platforms?
- Evidence of staff training on online safety and current risks?
- Annual review date and process?

If you've ticked most of these, your policy is on track for 2026.

References

[1] Department for Education. (2025). *Relationships education (Primary)*. GOV.UK. https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education

[2] Department for Education. (2025). *Keeping children safe in education 2025*. GOV.UK. https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

[3] PSHE Association. (2025). *The new statutory RSHE guidance: what's changed and what does this mean for primary schools*. https://pshe-association.org.uk/news/the-new-statutory-rshe-guidance-whats-changed-and-what-does-this-mean-for-primary-schools