KING'S STANLEY C OF E PRIMARY SCHOOL

WHERE WE CARE ABOUT LEARNING AND EACH OTHER

King's Stanley C of E Primary School Online Safety Policy
Written by: Mr van den Broek
Reviewed: May 2026
Next Review May 2028

1. Introduction

At King's Stanley C of E Primary School, digital technology is an integral part of learning and everyday life. This policy sets out how we promote the safe, responsible and effective use of technology and protect all members of the school community online.

We recognise that online technologies present both educational benefits and safeguarding risks. We are committed to ensuring that pupils develop the knowledge, skills and behaviours required to stay safe online.

Online safety is a key part of our safeguarding responsibilities and is embedded across all areas of school life.

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Acceptable Use Policy
- Behaviour Policy
- Data Protection Policy
- *Keeping Children Safe in Education (KCSIE)*

2. Whole School Approach

Online safety is a shared responsibility across the school community.

- The Governing Body provides strategic oversight and ensures appropriate systems are in place
- The Headteacher and Senior Leaders ensure effective implementation
- The Designated Safeguarding Lead (DSL) has overall responsibility for online safety and safeguarding
- The Computing Leader supports curriculum delivery and staff development
- All staff model safe and professional behaviours

All staff receive regular training **and updates** on online safety and emerging risks.

3. Online Safety in the Curriculum

Online safety is embedded across the curriculum, including computing and PSHE.

Pupils are taught to:

- use technology safely, respectfully and responsibly
- recognise risks such as grooming, exploitation, cyberbullying and harmful content
- understand online behaviour, including respectful communication

- critically evaluate information, including misinformation and fake content
- understand the legal and ethical implications of online actions

Teaching also covers:

- child-on-child abuse
- extremist content
- self-harm related material
- live streaming and social media risks

Pupils are taught how and where to seek help, both in school and beyond.

4. Artificial Intelligence (AI)

The school recognises the increasing use of AI technologies.

- AI tools may be used where appropriate for educational purposes
- Staff must not input personal, confidential or sensitive data into AI systems
- All AI-generated content must be checked for accuracy, bias and suitability
- AI must not replace professional judgement
- Pupils are taught to use AI tools critically, safely and responsibly

5. Managing Internet Access

The school provides a filtered and monitored internet service to safeguard users.

- Access is controlled through appropriate filtering systems
- All internet use is monitored to support safeguarding
- Monitoring is proportionate, lawful and understood by users
- Staff must preview websites and resources before use
- Pupils access the internet under appropriate supervision

Users must:

- report inappropriate content immediately
- close any unsuitable material without delay

6. Filtering and Monitoring

The school meets the DfE Filtering and Monitoring Standards.

- Systems are agreed by leaders, governors and the IT provider
- Provision is reviewed at least annually
- The DSL leads safeguarding oversight
- The IT provider manages technical systems

Filtering:

- blocks illegal and harmful content
- uses regularly updated content lists
- provides age-appropriate access
- includes reporting routes for concerns

Monitoring:

- covers all devices and network use
- identifies safeguarding risks through alerts
- is reviewed and acted upon promptly by the DSL
- supports early identification of concerns

7. Communication and Email

Staff must use approved school systems for communication.

- No use of personal email, social media or messaging apps with pupils or parents
- Email is monitored and should not be considered private

- Pupils may use school email systems only under supervision

Any concerning communication must be reported immediately.

8. Social Media and Online Communication

- Pupils are discouraged from using social media platforms below age limits
- Staff must maintain professional boundaries at all times
- Communication must occur only through approved school platforms

9. Use of Images and Media

The school uses images in line with safeguarding and data protection requirements.

- Consent is obtained and recorded on entry to school
- Consent is checked before use
- Parents may withdraw consent at any time
- Pupils are not identified by full name alongside images

Images must:

- be taken on school devices (unless authorised)
- be stored securely on school systems
- not be shared via personal devices or accounts

10. Mobile Phones and Personal Devices

Clear expectations are in place for device use.

- Pupils do not use phones during the school day
- Staff phones must not be used in view of pupils
- Devices must be stored securely during teaching time
- Additional care is taken on trips and off-site visits

Personal devices must not be used to store or access school data unless authorised.

11. Data Protection

The school processes personal data in line with UK GDPR and the Data Protection Act 2018.

- Data is accessed and stored using approved school systems only
- Staff must protect personal data at all times
- Personal devices or cloud services must not be used unless authorised

All data protection requirements are detailed in the Data Protection Policy.

12. Responding to Online Safety Concerns

All concerns must be taken seriously and responded to promptly.

Reporting procedures:

- All incidents must be recorded on CPOMS
- Urgent safeguarding concerns must be reported immediately to the DSL in person
- Concerns should never be delayed

Incidents may include:

- exposure to inappropriate material
- cyberbullying
- safeguarding risks
- breaches of policy

Serious incidents may involve:

- senior leadership
- external agencies
- the police

13. Cyberbullying

Cyberbullying is taken seriously and addressed in line with the Behaviour Policy.

Pupils are taught:

- how to recognise cyberbullying
- how to report concerns
- how to support others

All incidents are:

- recorded
- investigated
- addressed appropriately

14. Working with Parents and Carers

The school works in partnership with parents to promote online safety.

We provide:

- guidance and updates
- signposting to trusted resources
- support where concerns arise

Parents are encouraged to:

- monitor home internet use
- reinforce safe behaviours
- communicate concerns to the school

15. Monitoring, Review and Governance

- The Governing Body monitors the effectiveness of this policy
- Filtering and monitoring systems are reviewed regularly
- This policy is reviewed annually or in response to change