



Online Safety, Acceptable Use and Mobile Phone Policy

At Sherborne St John C of E Primary School, our policies are designed to ensure that every child can **achieve** their full potential, **enjoy** their learning, and be **inspired** by their experiences. This policy is underpinned by our core Christian values of **Trust, Truth and Forgiveness**, which enable us to build a secure, loving and thriving environment for our entire school community.

In line with our vision, this policy seeks to:

- **Foster Trust:** Building strong relationships with one another and exploring our relationship with God.
- **Uphold Truth:** Inspiring integrity and the courage to stand up for what is right.
- **Practice Forgiveness:** Creating an environment of patience and understanding where we take responsibility for our choices and move forward together when things go wrong.

Rooted in the Christian faith and the teachings of the Bible, our school remains a caring community where every individual is safe in the knowledge that they are loved and valued by God.

Date Adopted: October 2026

Review Date: October 2028

Responsible Committee: Governing Body / Safeguarding Committee

Policy Lead: Headteacher / Designated Safeguarding Lead

1. Policy Statement

At Sherborne St John C.E. Primary School, we are committed to creating a safe, healthy and positive learning environment where children can thrive academically, socially and emotionally.

The school recognises the growing concerns regarding children's exposure to smartphones, social media, online harms and excessive screen time. In support of the principles promoted by the Smartphone Free Childhood movement, the school seeks to minimise unnecessary access to internet-enabled mobile devices during the primary school years.

This policy sets out expectations regarding:

- Online safety and digital citizenship.
- Appropriate use of school technology.
- Mobile phones and smart devices.
- Responsibilities of pupils, staff and parents.



Online Safety, Acceptable Use and Mobile Phone Policy

- Procedures for managing breaches of the policy.

2. Aims

This policy aims to:

- Protect pupils from online risks and inappropriate content.
- Promote healthy relationships with technology.
- Support children's wellbeing, concentration and social development.
- Encourage responsible digital behaviour.
- Provide clear expectations regarding mobile phones and smart devices.
- Support parents in delaying smartphone ownership where possible.
- Ensure compliance with safeguarding, data protection and behaviour policies.

3. Smartphone Free School Commitment

Sherborne St John C.E. Primary School is committed to being a smartphone-free primary school.

The school believes that primary-aged children benefit from:

- Face-to-face friendships.
- Outdoor play and physical activity.
- Reduced exposure to social media.
- Better focus and concentration in learning.
- Protection from online harms.
- Improved emotional wellbeing.

Accordingly, smartphones are not permitted on the school site except in exceptional circumstances authorised by the Headteacher.

4. Mobile Phones and Smart Devices

4.1 Prohibited Devices

Pupils must not bring the following devices onto school premises:

- Smartphones.
- Internet-enabled mobile phones.
- Tablets and iPads.
- Smartwatches with messaging, internet, camera or communication functions.



Online Safety, Acceptable Use and Mobile Phone Policy

- Any device capable of accessing social media platforms.
- Any device capable of recording photographs, video or audio without school authorisation.

If brought onto site, these devices will be treated as unauthorised items.

4.2 Exceptional Permission for Basic Mobile Phones

The school recognises that a small number of Year 6 pupils may walk to and from school independently.

Only these pupils may be permitted to bring a mobile phone where:

- Written parental permission has been provided.
- The Headteacher has approved the request.
- The device is a basic "brick phone" capable only of voice calls and text messaging.
- The device has no internet connectivity, camera functions, social media apps or gaming capability.

Permission may be withdrawn at any time if the policy is breached.

4.3 Arrival Procedures

Where permission has been granted:

- The phone must be switched off before entering the school grounds.
- The phone must not be used anywhere on the school site.
- The phone must be handed to the class teacher or school office immediately upon arrival.
- The phone will be stored securely throughout the school day.

4.4 End of Day Procedures

- Phones will remain securely stored throughout the school day.
- Phones will be returned only at the end of the day when pupils leave school.

The school accepts no liability for loss or damage to devices brought onto site.

4.5 Medical Exemptions

The school recognises that some pupils may require technology to support medical needs.

Examples include:



Online Safety, Acceptable Use and Mobile Phone Policy

- Continuous glucose monitoring systems.
- Medical monitoring devices.
- Approved communication aids.

Any exemption must:

- Be discussed with the Headteacher and SENDCo.
- Be supported by relevant medical documentation.
- Form part of the pupil's healthcare plan where appropriate.

5. Unauthorised Devices and Enforcement

5.1 Confiscation

If a pupil is found in possession of an unauthorised device:

- The device will be confiscated immediately.
- It will be secured in the school office.
- Parents/carers will be informed.

5.2 Return of Devices

Confiscated devices will not normally be returned directly to pupils.

A parent or carer must arrange collection from the school office.

5.3 Repeated Breaches

Repeated breaches may result in:

- Meetings with parents.
- Behaviour sanctions in accordance with the Behaviour Policy.
- Withdrawal of permission to bring any mobile device.
- Further safeguarding actions where necessary.

5.4 Searches

Where staff have reasonable grounds to suspect that a prohibited device is being concealed, the school may exercise its powers under current education legislation and school searching procedures.



Online Safety, Acceptable Use and Mobile Phone Policy

Any searches will be carried out lawfully, proportionately and with regard to the welfare and dignity of the child.

6. Acceptable Use of School Technology

The school provides access to technology to support teaching and learning.

All pupils are expected to use school technology responsibly.

Pupils Must:

- Use devices only when instructed by staff.
- Use technology for educational purposes.
- Keep passwords secure.
- Respect others online.
- Follow adult instructions at all times.
- Report concerns immediately

Pupils Must Not:

- Access inappropriate websites.
- Attempt to bypass security systems or filtering software.
- Download unauthorised applications.
- Alter device settings.
- Access another person's account.
- Create or share offensive material.
- Record images, videos or audio without permission.

School Devices

School-owned laptops, Chromebooks and tablets are provided to support learning.

The school reserves the right to:

- Monitor usage.
- Restrict access.
- Review browsing records where safeguarding concerns arise.

Deliberate damage to school equipment may result in parents being asked to contribute towards repair or replacement costs



Online Safety, Acceptable Use and Mobile Phone Policy

7. Online Safety Standards

Sherborne St John C.E. Primary School teaches online safety as part of its curriculum and safeguarding responsibilities.

Pupils are taught to:

- Stay safe online.
- Think critically about information they see.
- Recognise scams and online risks.
- Treat others respectfully.
- Seek help when worried.

Reporting Concerns

Pupils must immediately report:

- Inappropriate images.
- Harmful content.
- Disturbing messages.
- Online bullying.
- Contact from unknown individuals.
- Any activity that makes them feel uncomfortable or worried.

Reports should be made to:

- A class teacher.
- The Designated Safeguarding Lead.
- Another trusted adult in school

Personal Information

Pupils must never share:

- Home address.
- Personal telephone numbers.
- Passwords.
- School location details.
- Personal photographs.
- Financial information.



Online Safety, Acceptable Use and Mobile Phone Policy

Unless specifically authorised by staff and parents.

Cyberbullying

The school has zero tolerance for cyberbullying.

Cyberbullying includes:

- Sending unkind messages.
- Excluding others online.
- Sharing rumours digitally.
- Posting harmful comments.
- Creating fake profiles.

Incidents may be sanctioned even where behaviour originates outside school if it affects pupils' wellbeing, safety or learning.

8. Social Media

Pupils must not access social media during the school day.

School internet systems are configured to block access to social networking and other unsuitable sites wherever possible.

The school strongly encourages families to follow age restrictions for social media platforms and messaging services.

9. Expectations for Parents and Carers

Parents and carers play a vital role in supporting children's digital wellbeing.

The school encourages families to:

- Delay smartphone ownership for as long as possible.
- Consider basic mobile phones as a safer alternative.
- Monitor online activity at home.
- Use parental controls.
- Set healthy screen time boundaries.
- Discuss online safety regularly.



Online Safety, Acceptable Use and Mobile Phone Policy

Parent Smartphone-Free Pledge

The school supports community initiatives that encourage families to:

- Delay smartphone ownership until at least age 14 where possible.
- Delay social media access until the minimum legal platform age requirements are met.
- Promote healthy childhood development through reduced screen exposure.

Photography on Site

To safeguard all children:

- Parents should avoid using mobile phones on the playground and school premises.
- Photography and filming may only take place during authorised school events.
- Images must not be shared on social media without consent.

Online Issues Outside School

The school may offer advice and support regarding online issues occurring outside school hours.

However, parents retain primary responsibility for:

- Online activity at home.
- Device management.
- Social media use.
- Messaging services.
- Gaming platforms.

Where external online issues have a significant impact on a child's safety, wellbeing or education, the school may take appropriate safeguarding action.

10. Monitoring and Review

This policy will be reviewed annually by the Headteacher and Governing Body, or sooner if required by changes in legislation, safeguarding guidance or school practice.

Agreement



Online Safety, Acceptable Use and Mobile Phone Policy

By attending Sherborne St John C.E. Primary School, pupils and parents agree to support and comply with this Online Safety, Acceptable Use and Mobile Phone Policy in order to help maintain a safe, respectful and smartphone-free school environment for all members of the community.

12. Filtering, Monitoring and Digital Safeguarding

Commitment to Safe Online Access

Sherborne St John C.E. Primary School recognises that online safety is a safeguarding issue and that effective filtering and monitoring systems form a key part of the school's child protection arrangements.

In accordance with Keeping Children Safe in Education (KCSIE) and the DfE Filtering and Monitoring Standards, the school will maintain appropriate filtering and monitoring systems to safeguard pupils from harmful, inappropriate or illegal online content whilst supporting effective teaching and learning.

The school acknowledges that no filtering or monitoring system can provide complete protection and therefore combines technical controls with education, supervision, staff training and effective safeguarding procedures.

Filtering

The school's filtering system will be designed to:

- Block access to illegal content.
- Prevent access to child sexual abuse material and other unlawful content.
- Restrict access to pornography and sexually explicit material.
- Restrict access to extremist, radicalising or terrorist content.
- Restrict gambling websites.
- Restrict content promoting self-harm, suicide, eating disorders or other harmful behaviours.
- Restrict access to social media and messaging services where appropriate.
- Protect users from phishing, malware and cyber-security threats.
- Support age-appropriate access to online resources for learning.

Monitoring

The school operates monitoring systems designed to identify potential safeguarding concerns and inappropriate use of school technology.

Monitoring may include:



Online Safety, Acceptable Use and Mobile Phone Policy

- Internet browsing activity.
- Searches conducted on school systems.
- User account activity.
- Attempts to access blocked or inappropriate content.
- Indicators of cyberbullying.
- Searches or behaviours that may indicate a safeguarding concern.
- Attempts to bypass filtering or security controls.

Monitoring systems are not used to routinely "spy" on pupils but to identify risks, support safeguarding and protect users.

Online Safety and Safeguarding Concerns

Where filtering or monitoring systems identify concerns, the school will consider whether the activity may indicate:

- Bullying or cyberbullying.
- Child-on-child abuse.
- Harmful sexual behaviour.
- Mental health concerns.
- Radicalisation or extremism.
- Online grooming.
- Exploitation.
- Exposure to harmful content.
- Other safeguarding concerns.

Concerns will be managed through the safeguarding procedures outlined in the Child Protection and Safeguarding Policy.

Governance and Oversight

The Governing Body will receive regular assurances that:

- Filtering and monitoring systems are effective.
 - Appropriate safeguarding responses are in place.
 - Risks are reviewed regularly.
 - Staff understand their responsibilities.
 - All statutory requirements are met.
-



Online Safety, Acceptable Use and Mobile Phone Policy

13. Artificial Intelligence (AI), Emerging Technologies and Online Content

Use of Artificial Intelligence

The school recognises the increasing availability of Artificial Intelligence (AI) technologies, including generative AI tools, chatbots, image generators and automated online services.

Whilst AI may provide educational opportunities, it may also create safeguarding, privacy and misinformation risks.

The school will ensure that any AI technologies used within school are:

- Age-appropriate.
- Educationally justified.
- Risk assessed where appropriate.
- Compliant with data protection requirements.
- Used under appropriate supervision.

Teaching Pupils About AI

As part of online safety education, pupils will be taught that:

- AI-generated information may not always be accurate.
- AI systems can generate false, misleading or biased content.
- Images, videos and audio may be manipulated using AI.
- Not everything online should be trusted without verification.
- Personal information should never be shared with AI tools or online platforms without adult permission.

Pupils will be encouraged to develop critical thinking skills when engaging with online content and emerging technologies.

Deepfakes and Manipulated Content

The school recognises that AI technology can create realistic but false images, audio and video content, commonly referred to as "deepfakes".

Pupils will be taught to:

- Question the authenticity of digital content.



Online Safety, Acceptable Use and Mobile Phone Policy

- Seek help if they encounter concerning material.
- Report content that appears misleading, harmful or upsetting.
- Understand that creating or sharing manipulated content intended to deceive, embarrass or harm others may result in sanctions and safeguarding action.

Appropriate Use of AI by Pupils

Pupils must not:

- Use AI tools to access inappropriate content.
- Generate harmful, offensive, discriminatory or abusive material.
- Create images, videos or audio designed to humiliate, bully or deceive others.
- Use AI to impersonate another person.
- Submit AI-generated work as their own without permission from staff.
- Use AI to bypass learning activities, assessments or school expectations.
- Share personal data, photographs or identifying information with AI platforms.

Staff Use of Artificial Intelligence

Staff may use approved AI tools to support teaching, administration and professional practice where appropriate.

Staff must:

- Follow all data protection and GDPR requirements.
- Not enter confidential, personal or sensitive school information into public AI systems.
- Critically review AI-generated outputs for accuracy and suitability.
- Consider safeguarding, bias and equality implications when using AI-generated content.
- Follow any school guidance relating to the safe and ethical use of AI.

Any AI-generated resources used with pupils must remain appropriate to the age, developmental stage and needs of the children concerned.

Additional DSL Responsibility

Under Section 14, I would add the following responsibility to the DSL role:



Online Safety, Acceptable Use and Mobile Phone Policy

Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- Responding to online safety concerns.
- Managing safeguarding incidents involving technology.
- Supporting staff and families.
- Monitoring emerging online risks.
- Keeping abreast of developments in technology, social media, gaming platforms and artificial intelligence.
- Ensuring that technology-related safeguarding risks are reflected within safeguarding training, procedures and risk assessments.
- Working with school leaders to ensure filtering, monitoring and online safety arrangements remain effective and compliant with statutory guidance.

