Bledington Primary School

DIGITAL COMMUNICATION, MOBILE DEVICES AND SOCIAL MEDIA POLICY

Date of Policy	*Date of ratification by Governing Body*	**Signed:** **COHEADTEACHERS** **Jill Kewley & Amanda Ziebeck** **COCHAIRS OF GOVERNORS** *K Dainty A Hammerstein*
17.08.26	***07.10.26***	

Safeguarding Statement

At Bledington Primary School we respect and value all children and are committed to providing a caring, friendly and safe environment for all our pupils so they can learn, in a relaxed and secure atmosphere. We believe every pupil should be able to participate in all school activities in an enjoyable and safe environment and be protected from harm. This is the responsibility of every adult employed by, or invited to deliver services at Bledington Primary School. We recognise our responsibility to safeguard all who access school and promote the welfare of all our pupils by protecting them from physical, sexual and emotional abuse, neglect and bullying.

1. Policy Aims

This policy combines and replaces the school's Mobile Phone Policy and Social Media Policy and supports our Acceptable Use policy..

The aims are to:

- Safeguard children from harm.
- Promote safe, responsible and professional use of digital technologies.
- Maintain professional boundaries between staff, pupils and parents.
- Protect personal data and confidentiality.
- Prevent online bullying, harassment and abuse.
- Protect the reputation of pupils, families, staff and the school.
- Ensure compliance with safeguarding and data protection legislation.
- Provide clear expectations regarding mobile phones, social media, messaging services, AI tools and other digital technologies.

---

2. Related Policies and Guidance

This policy should be read alongside:

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Online Safety Policy
- Acceptable Use Agreements
- Behaviour Policy
- Anti-Bullying Policy
- Complaints Policy
- Data Protection Policy
- Photography and Video Consent Procedures
- KCSIE (latest version)
- Data Protection Act 2018 and UK GDPR
- Online Safety Act 2023
- DfE Filtering and Monitoring Standards

---

3. Scope

This policy applies to:

- Staff
- Governors
- Volunteers
- Contractors
- Visitors
- Parents and carers
- Pupils

It covers:

- Mobile phones
- Smartphones
- Smart watches
- Tablets
- Laptops
- Cameras
- Messaging applications
- Social media platforms
- Artificial intelligence tools
- Any internet-enabled device

---

4. General Principles

All users must:

- Act professionally and respectfully.
- Protect children's welfare at all times.
- Respect confidentiality.
- Follow school safeguarding procedures.
- Protect personal and school data.
- Use technology in ways that uphold the school's values.

No technology should ever be used to:

- Bully, intimidate or harass.
- Share confidential information.
- Circumvent safeguarding procedures.
- Damage the reputation of individuals or the school.
- Access inappropriate content.

---

5. Staff Use of Mobile Phones and Personal Devices

During School Hours

Staff must:

- Keep personal devices on silent mode.
- Store devices out of sight when pupils are present.
- Limit personal use to breaks and non-contact time.
- Ensure personal use does not interfere with professional duties.

Staff must not:

- Use personal devices while supervising children.
- Make personal calls during teaching time except in emergencies.
- Text, email or use social media during contact time.
- Use personal devices in classrooms, playgrounds or other pupil areas unless authorised by the CoHeadteachers..

Emergency Circumstances

Staff with exceptional personal circumstances may keep a phone accessible only with CoHeadteachers approval.

---

6. Photography, Video and Audio Recording

For safeguarding reasons:

Staff must not (unless authorised by the CoHeadteachers):

- Photograph pupils using personal devices.
- Film pupils using personal devices.
- Create audio recordings of pupils using personal devices.
- Store pupil images on personal equipment.

All images must be stored in accordance with school data protection procedures.

7. Professional Communication

Communication with parents must take place through approved school systems:

Examples include:

- School email
- School telephone systems
- School-approved messaging platforms
- School website
- Official school social media channels

Staff must not:

- Use personal telephone numbers for routine communication.
- Use personal WhatsApp accounts with parents.
- Use personal social media messaging systems with parents.
- Share private contact details.

8. Staff Social Media Expectations

Staff are entitled to private online lives but must recognise their professional responsibilities.

Staff must:

- Maintain appropriate privacy settings.
- Consider the professional impact of online activity.
- Safeguard confidential information.

Staff must not:

- Post information about pupils.
- Post photographs of pupils.
- Post information about colleagues without consent.
- Discuss confidential school matters online.
- Criticise pupils, parents, staff or governors online.
- Bring the school into disrepute.

Staff should exercise caution when identifying themselves as employees of the school on personal social media accounts.

9. Relationships with Pupils Online

Staff must not:

- Accept friend requests from current pupils.
- Follow current pupils using personal accounts.
- Message current pupils through personal platforms.
- Share personal social media details with pupils.

Where contact is attempted by a pupil:

- The request must be declined.
- The CoHeadteachers should be informed.
- A record should be made if appropriate.

10. Artificial Intelligence (AI)

AI technology is increasingly used within education.

Examples include:

- Microsoft Copilot
- ChatGPT
- Gemini
- Claude
- Other generative AI systems

Staff who use AI for professional purposes must:

- Check all outputs for accuracy.
- Review content for bias and appropriateness.
- Ensure safeguarding considerations are met.
- Verify information before use with pupils.

Staff must not:

- Enter confidential pupil information into public AI tools.
- Upload personal data unless the platform has been approved and assessed for GDPR compliance.
- Rely solely on AI-generated content without professional judgement.

- AI-generated content must not be used for safeguarding decisions, SEND assessments, disciplinary decisions, or any high-risk decision without appropriate professional review and oversight.

---

11. Cyber Security and Data Protection

All members of staff must:

- Use strong passwords.
- Protect login credentials.
- Lock devices when unattended.
- Report cyber security concerns immediately.
- Follow school data protection procedures.

Where available, multi-factor authentication should be enabled.

Suspected:

- phishing emails
- hacking attempts
- malware incidents
- data breaches

must be reported immediately to the CoHeadteachers.

---

12. Remote Working Expectations

A growing safeguarding and GDPR issue.

Suggested wording:

When working remotely, staff must take reasonable steps to ensure screens, documents and online meetings cannot be viewed or overheard by unauthorised individuals.

13.Pupils

Mobile Phones

Pupils are generally not permitted to bring mobile phones into school.

Where exceptional permission is granted:

- Parents must seek prior approval.
- Phones must be switched off.
- Phones must be handed to a designated member of staff.
- Devices remain the responsibility of the owner.

Smart Watches

In school, pupils may not use smart watches with:

- messaging functions
- internet access
- photography capabilities
- audio recording function.

Social Media

Pupils must not:

- Access social media during the school day.
- Use social media via school devices unless directed by staff for educational purposes.
- Make harmful or inappropriate comments about members of the school community.

---

13. Parents and Carers

The school values positive relationships with parents and carers.

Parents and carers are expected to:

- Communicate respectfully.
- Raise concerns through official channels.
- Support safe online behaviour.

Parents must not:

- Post images of other children online without consent.
- Publish material that identifies other pupils.
- Use social media to harass or intimidate members of the school community.
- Share misinformation relating to school matters.

Concerns should be raised through:

- The class teacher
- The CoHeadteachers

- The Complaints Policy

rather than through social media.

---

14. Volunteers, Governors, Visitors and Contractors

All visitors must follow the same expectations regarding:

- mobile phones
- photography
- video recording
- social media use

Visitors must not photograph or record children under any circumstances unless authorised by the CoHeadteachers.

---

15. Educational Visits

Staff, volunteers and parents supporting trips must:

- Follow this policy at all times.
- Avoid social media use during visits.
- Use school communication procedures only.

Photographs must only be taken on approved school equipment.

---

16. Online Bullying and Inappropriate Use

Online bullying includes:

- abusive messages
- threatening messages
- sharing images without consent

- impersonation
- malicious rumours
- exclusion from online groups

All incidents will be investigated in line with school safeguarding and behaviour procedures.

Where necessary the school may involve:

- parents
- governors
- local authority services
- police
- social care

---

17. Breaches of this Policy

Breaches may result in:

For staff:

- Informal management action
- Formal disciplinary procedures
- Referral to professional bodies
- Referral to external agencies

For pupils:

- Behaviour sanctions
- Restriction of digital access
- Parental involvement
- Safeguarding intervention

For visitors and parents:

- Withdrawal of permission to enter the site
- Formal complaints procedures
- Legal action where appropriate

---

18. Monitoring and Review

The CoHeadteachers and Governing Body will monitor implementation of this policy.

The policy will be reviewed:

- Annually
- Following legislative changes
- Following significant safeguarding incidents
- Following DfE guidance updates