Bledington Primary School

Acceptable Use, Online Safety and Digital Communications Policy

Policy and Guidance on School Staff and pupils' use of ICT and Communications Systems

Please also refer to our Safeguarding, Equal opportunities, Behaviour, Anti-bullying, Confidentiality, Social media, Mobile phone and Health and Safety and Remote learning policy for the North Cotswold Cluster.

This policy should be read in conjunction with Keeping children safe in education
Keeping children safe in education (publishing.service.gov.uk)

All policies are available on the school website
http://www.bledington.gloucs.sch.uk/policies/

Date of Ratification by Governors: 31.03.17 24.01.19 23.09.21 22.09.22 12.10.23 04.07.24 09.07.25 07.10.26	*Updated* *04.12.18* *02.02.21* *14.09.21* *08.08.22* *15.08.23* *25.06.24* *01.07.25*	**Signed:** **CO-HEADTEACHERS:** **Jill Kewley & Amanda Ziebeck** **CO-CHAIRS OF GOVERNORS** *K Dainty A Hammerstein*

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.

Review Frequency: Annually or sooner following changes to legislation, statutory guidance, safeguarding requirements or DfE digital standards.

This policy should be read in conjunction with:

- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children 2023
- UK GDPR and the Data Protection Act 2018
- The Prevent Duty Guidance
- DfE Meeting Digital and Technology Standards: Filtering and Monitoring
- School Safeguarding, Online Safety, Staff Code of Conduct, Mobile Phone, Behaviour, Anti-Bullying, Data Protection and Social Media Policies.

POLICY STATEMENT

The Governing Body at Bledington Primary School recognises the use of its ICT and communications facilities as an important resource for teaching, learning and personal development and as an essential aid to business efficiency. It actively encourages staff to take full advantage of the potential for ICT and communications systems to enhance development in all areas of the curriculum and school administration. It is also recognised by the Governing Body that along with these benefits there are also responsibilities, especially for ensuring that pupils are protected from contact with inappropriate material.

In addition to their normal access to the school's ICT and communications systems for work-related purposes, the Governing Body permits staff limited reasonable personal use of ICT equipment and email and internet facilities during their own time subject to such use:

1. Not depriving pupils of the use of equipment
2. Not interfering with the proper performance of the staff member's duties

Whilst the school's ICT systems may be used for both work-related and for sole personal use, the Governing Body expects use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of the Governing Body at all times.

This policy document is issued to all staff before they are provided with laptops, tablets, cameras, USB / portable hard drive devices, mobile phones and passwords giving access to the ICT network.

Policy coverage

This policy covers the use by staff of all school-owned ICT and communications equipment, examples of which include:

- Laptops, tablets and personal computers;
- ICT network facilities;

- Personal digital organisers and handheld devices;
- Mobile phones and phone/computing hybrid devices;
- USB keys and other physical and on-line storage devices;
- Image data capture and storage devices including cameras, camera phones and video equipment.

This list is not exhaustive.

The policy covers the use of all ICT and communications equipment provided for work purposes and equipment which is on loan to staff by the school for their sole personal use. An agreement is to be signed (Appendix 2)

Online Safety

The School recognises that online safety is a safeguarding issue and a whole-school responsibility.

Online risks include:

- Content: exposure to harmful, illegal or inappropriate material.
- Contact: harmful interactions with adults or peers.
- Conduct: unsafe or inappropriate online behaviour.
- Commerce: scams, phishing, fraud, gambling and financial exploitation.

The School will maintain appropriate filtering and monitoring systems, review them at least annually and ensure safeguarding and IT leads work together effectively.

Artificial Intelligence (AI)

Staff and pupils may only use AI tools that have been approved by the School.

Users must not:

- enter personal, confidential or safeguarding-related information into public AI systems;
- use AI to generate offensive, harmful or discriminatory content;
- present AI-generated work as wholly their own where this would constitute academic dishonesty.

The School will consider AI-related risks when reviewing filtering and monitoring arrangements.

Data Protection

All staff must:

- comply with UK GDPR and the Data Protection Act 2018;

- only process personal data where necessary and lawful;
- use school-approved systems for storing personal information;
- report any actual or suspected data breach immediately to the Headteacher and Data Protection Officer;
- ensure personal data is transferred securely.

Staff must not use personal email accounts to store or transfer confidential school information unless expressly authorised.

Cyber Security

Staff must:

- use strong passwords and multi-factor authentication where available;
- lock devices when unattended;
- ensure devices receive security updates;
- report suspicious emails, phishing attempts or cyber incidents immediately;
- not circumvent security controls.

The School will work towards meeting DfE Cyber Security Standards for Schools and Colleges.

The use of Bledington School ICT and Communications Facilities including Teams

Staff who use the school's ICT, Teams and communications systems:

- Must use it responsibly;
- Must keep it safe;
- Must not share and treat as confidential any passwords provided to allow access to ICT equipment and/or beyond firewall protection boundaries;
- Must report any known breach of password confidentiality to the CoHeadteachers or nominated ICT Co-ordinator as soon as possible;
- Must report known breaches of this policy, including any inappropriate images or other material which may be discovered on the school's ICT systems;
- Must report to the CoHeadteachers, any vulnerabilities affecting child protection/ safeguarding in the school's ICT and communications systems;
- Must not install software on the school's equipment, including freeware and shareware, unless authorised to do so by the school's ICT Co-ordinator;
- Must comply with any ICT security procedures governing the use of systems in the school, including anti-virus measures;

- Must ensure that it is used in compliance with this policy.

Any equipment provided to a member of staff is provided for their sole personal use. Use of the equipment by family or friends is **not** permitted and any misuse of the equipment by unauthorised users will be the responsibility of the staff member.

Whilst it is not possible to cover all eventualities, the following information is published to guide staff on the expectations of the Governing Body. Any breaches of this policy or operation of the school's equipment outside statutory legal compliance may be grounds for disciplinary action being taken.

Email and Internet and Communications systems usage

The following use of the school's ICT system is strictly prohibited and may amount to gross misconduct. (This could result in dismissal):

1. To make, to gain access to, or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read or see it;
2. To make, to gain access to, and/or for the publication and distribution of material promoting homophobia or racial or religious hatred;
3. For the purpose of bullying or harassment, or in connection with discrimination or denigration on the grounds of gender, race, religious, disability, age or sexual orientation;
4. For the publication and/or distribution of libellous statements or material which defames or degrades others;
5. For the publication of material that defames, denigrates or brings into disrepute the school and/or its staff and pupils;
6. For the publication and distribution of personal data without authorisation, consent or justification;
7. Where the content of the email correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination;
8. To participate in on-line gambling;
9. Where the use infringes copyright law;
10. To gain unauthorised access to internal or external computer systems (commonly known as hacking);
11. To create or deliberately distribute ICT or communications systems "malware", including viruses, worms, etc;
12. To record or monitor telephone or email communications without the express approval of the Governing Body (or the Chair of Governors). In no case will such recording or monitoring be permitted unless it has been established for that such action is in full compliance with all relevant legislation and regulations. Monitoring and access to communications will be conducted in

accordance with applicable legislation, including:

- UK GDPR
- Data Protection Act 2018
- Investigatory Powers Act 2016
- Human Rights Act 1998

Any monitoring undertaken by the School will be proportionate, justified, documented and limited to legitimate safeguarding, security, operational or legal purposes.

13. To enable or assist others to breach the governors' expectations as set out in this policy.

Additionally, the following uses of school ICT facilities are not permitted and could lead to disciplinary action being taken:

1. For participation in "chain" email correspondence (including forwarding hoax virus warnings);
2. In pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade unions);
3. To access ICT facilities by using another person's password, or to post anonymous messages or forge email messages using another person's identity.

This policy applies to email, messaging applications, social networking services, online gaming platforms and collaboration tools including but not limited to Microsoft Teams, WhatsApp, Instagram, Snapchat, TikTok, Facebook, X, YouTube, Discord and any future social media platform.

Filtering & Monitoring responsibilities

The Designated Safeguarding Lead (DSL), Headteacher and those responsible for ICT will work together to:

- oversee filtering and monitoring arrangements;
- review filtering and monitoring effectiveness annually;
- respond to safeguarding concerns generated through monitoring systems;
- provide assurance to Governors that systems remain effective.

ADDENDUM: This policy has been written with reference to Keeping Children Safe in Education which states that the use of technology has become a significant component of many safeguarding issues and often provides the platform that

facilitates harm. Due to Covid-19 and the practice of Remote Learning, we recognise the importance of ensuring secure, filtered systems and the monitoring of e-safety procedures across the year groups. Where/When children are being asked to learn online at home the Department has provided advice to support schools and colleges do so safely: safeguarding in schools colleges and other providers and safeguarding and remote education. The NSPCC and PSHE Association also provide helpful advice: • NSPCC Learning - Undertaking remote teaching safely during school closures • PSHE - PSHE Association coronavirus hub.

An agreement for parents/carers who have borrowed school laptops has also been drawn up and is attached (Appendix 1) under the following important information:

Cyber Bullying Parents are made aware of the school's policy of access to social networking sites through this policy. Where a disclosure of cyber bullying is made, schools have a duty to investigate and protect, even where the bullying originates outside the school. Once a disclosure is made, investigation may have to involve the families. This should be dealt with under the school's 'Anti-bullying and Hate-crime policy.' If bullying continues, the incident(s) will be referred to the police as harassment. This guidance can apply to text and mobile phone cyber bullying.

Child Sexual Exploitation (CSE), Child Criminal Exploitation (CCE), County Lines activity, online grooming and technology-facilitated abuse.

Staff should remain alert to all forms of exploitation and report concerns in accordance with the BPS Safeguarding Policy.

The school, through its updated Safeguarding policy, identifies CSE via social media, IT or physically as a form of abuse. It is the abuse of a position of vulnerability, differential power, or trust for sexual purposes; this includes profiting monetarily, socially or politically from the exploitation of another (for example child prostitution and grooming of children for sexual abuse and exploitation). To that end, Staff should be aware of the signs that a child might be so abused. To that end, such incidents will be recorded as a safeguarding incident.
Child Exploitation and Online Centre: Gloucestershire Constabulary works closely with the Child Exploitation and Online Protection Centre (CEOP), which is a part of the National Crime Agency. Their website Thinkuknow offers advice and resources for young people, their parents and carers, teachers and trainers as well as a reporting tool https://www.thinkuknow.co.uk/
Safer Internet Centre: The UK Safer Internet Centre is coordinated by Childnet International, the Internet Watch Foundation and the Southwest Grid for Learning. They provide an awareness centre, a helpline for professionals working with children and a hotline where you can report online content that you are concerned may be of a criminal nature, for example indecent images of children.
Website: http://www.saferinternet.org.uk/about/helpline
Phone: 0844 381 4772
NSPCC : The NSPCC also offers advice for keeping your child safe online. Their 'Be Share Aware' campaign features films to show and discuss with your child on the issues of sharing explicit photos and personal information. https://www.nspcc.org.uk/

Please see below for appendices

Appendix 2
Parent agreement

BLEDINGTON SCHOOL
The School House,
Old Burford Road,
Bledington,
Chipping Norton,
Oxon. OX7 6US
01608658388

CoHeadteachers:
Ms Jill Kewley & Mrs Amanda Ziebeck
head@bledington.gloucs.sch.uk

1. This agreement is between:
1) Bledington Primary School ("the School") and

2) Name of parent: _____

Address: _____
(the "parent" and I)

And governs the care and use of the device assigned to the parent's child (the "pupil"). This agreement covers the period from the date the device is issued through to the return date of the device to the school.
All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1.The school is lending the pupil a laptop ("the equipment") for the purpose of doing school work from home.

2.This agreement sets the conditions for taking a Bledington School laptop ("the equipment") home.

Security

Parents must ensure:

- devices are protected by passwords;
- devices are used only by the named pupil;
- safeguarding restrictions and filtering systems are not removed or bypassed.

Data Protection

Parents and pupils must not:

- attempt to access other users' accounts;
- download software without permission;

- interfere with the school's security settings.

Monitoring

Parents acknowledge that activity on school-managed devices may be monitored, logged and reviewed for safeguarding, security and operational purposes.

I confirm that I have read the terms and conditions set out in this agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

2. Damage/loss

By signing this agreement, I agree to take full responsibility for the loan equipment issued to the pupil and I have read and understand the conditions of the agreement.

I understand that I and the pupil are responsible for the equipment at all times whether on the school's property or not.

If the equipment is damaged, lost or stolen, I will immediately inform Ms Kewley, and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use;
- Don't leave the device in a car or on show at home;
- Don't eat or drink around the device;
- Don't lend the device to siblings or friends;
- Don't leave the equipment unsupervised in unsecured areas.

3. Unacceptable use

I agree that my child will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to the following:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Causing intentional damage to ICT facilities or materials
- Using inappropriate or offensive language

4. Personal use
I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

5. Return date
I will return the device in its original condition and packaging to the school office within 7 days of being requested to do so.

I will ensure the return of the equipment to the school if the pupil no longer attends the school.

7. Consent
By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

Pupil's Name	
Device Serial Number	
Parent's Name	
Parent's Signature	
Date	

Appendix 2

Policy and Guidance on Bledington School use of ICT and Communications Systems

PART 1: to be retained by staff member

This declaration refers to the Governing Body's policy and guidance on the use of the school's ICT and communications systems and confirms that you have been provided with a copy and that you have agreed to follow it.

All employees, supply agency staff and, where appropriate, consultants, multi-agency staff, visitors, contractors, students and volunteers working in school are required to familiarise themselves with the contents of the policy on the use of ICT systems and sign the following declaration.

Declaration

You should sign two copies of this document; this copy to be retained by you. The second copy is to be detached and will be placed in your personnel file.

I confirm that I have been provided with a copy of the school's policy and guidelines on the use of the school's ICT and communications systems and I agree to the terms and conditions specified therein. I confirm that I am aware that all my electronic communications including emails and website searches may be monitored by the school and that this applies if I am working from home on school equipment or networks.

I have also read Bledington Primary Schools Digital Communications, Social Media policy and Mobile phone policy.

Signed: ..... Name: .....

Position Held: ..... Date: .....

Policy and Guidance on Bledington School use of ICT and Communications Systems

PART 2: to be detached and placed on the employee's file

This declaration refers to the Governing Body's policy and guidance on the use of the school's ICT and communications systems and confirms that you have been provided with a copy and that you have agreed to follow it.

All employees, supply agency staff and, where appropriate, consultants, multi-agency staff, visitors, contractors, students and volunteers working in school are required to familiarise themselves with the contents of the policy on the use of ICT systems and sign the following declaration.

Declaration

You should sign two copies of this document; this copy will be retained in your personnel file.

I confirm that I have been provided with a copy of the school's policy and guidance on the use of the school's ICT and communications systems and I agree to the terms and conditions specified therein. I confirm that I am aware that all my electronic communications including emails and website searches may be monitored by the school and that this applies if I am working from home on school equipment or networks.

I have also read Bledington Primary Schools Confidentiality, Social Media policy and the Mobile phone policy.

Signed: ..... Name: .....

Position Held: ..... Date:.....

Updated Annually