ACCEPTABLE USE POLICY

TO BE REVIEWED BY NOVEMBER 2026

Elmley Castle C of E First School School Vision

At Elmley Castle C of E First School, we believe that every child is a light in the world. We love one another, inspire growth, and serve our community with kindness. We embrace resilience, learning from our mistakes and growing stronger together. Each day, we strive to shine in all that we do, creating a safe and welcoming space where everyone can grow in faith, knowledge, and community. Together, we light the way for a brighter future, serving as beacons of hope and love to all.

"You are the light of the world. A city set on a hill cannot be hidden." – Matthew 5:14

BLISS
Believe in yourself
Love one another
Inspire greatness
Shine with kindness
Serve with a heart of compassion

Let your Light Shine!

1. Introduction

Elmley Castle CE First School provides access to computers, digital devices, networks, and online resources to enhance teaching, learning and professional activity. This policy outlines acceptable, safe and responsible use for all staff, pupils, governors and visitors in line with KCSIE 2025, UK GDPR, Prevent Duty, and national online safety expectations.

"The computer system" refers to all hardware, software, networks and digital services owned, leased, or used by the school, on-site or remotely.

Use of the school's systems must reflect our Christian vision: Let Your Light Shine—promoting kindness, responsibility, integrity and respect.

2. Acceptable Use Principles

All users must:

- Use technology in ways that keep themselves and others safe
- Protect personal data and follow GDPR requirements
- Use respectful, kind and professional communication at all times
- Report concerns immediately, including any safeguarding concerns relating to online behaviour or content
- Act in line with school values and the Staff Code of Conduct

Unacceptable use includes:

- Accessing or attempting to access inappropriate, illegal or harmful content
- Using school systems for personal financial gain, gambling, extremist material, political activity or advertising
- Installing unauthorised hardware or software
- Any activity that threatens the security, integrity or performance of school systems

The school reserves the right to monitor all digital activity on systems it owns or manages.

3. Internet Access (Pupils & Staff)

The school's internet access is provided through a filtered and monitored service via Worcestershire County Council.

Staff

- Staff have password-protected accounts that must not be shared.
- Internet use must be professional and aligned with school duties.
- Staff are responsible for emails sent and must use professional language.
- Accessing or sharing inappropriate sites or materials is strictly prohibited.

Pupils

Pupils may only access the internet:

- Under direct adult supervision
- With parental consent
- Through school-approved devices and platforms

Pupils are taught:

- How to stay safe online (age-appropriate online safety curriculum)
- What to do if they encounter inappropriate content (turn off/close the screen and tell an adult)

4. Monitoring and Filtering

The school uses:

- LA-managed filtering systems
- Monitoring software that flags harmful or inappropriate searches and content
- Termly reports reviewed by the Headteacher/Online Safety Lead

The school may:

- Check emails, internet history, files and logs
- Disable accounts if misuse is suspected
- Implement additional filtering when required

Serious breaches are recorded in the ICT Acceptable Use Log and may result in disciplinary action.

5. Use of School Devices & Portable Equipment

The school provides devices such as laptops, iPads and cameras for educational and professional use.

Users must:

- Take care of devices
- Keep devices password-protected
- Ensure devices are not left unsecured (e.g., visible in cars)
- Return devices when requested or when leaving employment

Staff may:

- Take laptops offsite for school work
- Connect to home WiFi

Staff must not:

- Install unapproved software
- Store sensitive data on personal devices

6. Email, Communication & Digital Conduct

All digital communication must be:

- Respectful
- Professional
- Aligned with school safeguarding and data protection policies

Staff must not:

- Use personal phones or emails to communicate with pupils
- Use school emails for inappropriate or unprofessional purposes
- Share confidential information without authorisation

Emails with inappropriate language may be automatically redirected for safeguarding review.

7. Online Publishing, Photos & Videos

To protect children and comply with safeguarding requirements:

- No pupil surname will be used online
- No photos/videos will be published without parental consent
- No content should identify a child's home location
- Staff must follow the school's Photograph & Video Policy and KCSIE guidance

Any concerns around publishing or identifying information must be shared immediately with the DSL.

8. Responding to Misuse

Breaches of this policy will be managed according to:

- Behaviour Policy (for pupils)
- Staff Disciplinary Policy
- Safeguarding & Child Protection Policy
- LA HR procedures

Sanctions may include:

- Restriction/removal of access
- Meetings with parents
- Formal disciplinary action
- Referral to external agencies where necessary

Illegal activities will be reported to the police.

9. Safeguarding & Online Safety

All online activity is subject to the school's safeguarding procedures. Users must:

- Report concerns immediately to the DSL
- Never engage in unprofessional online behaviour
- Understand the risks associated with online activity, including grooming, extremism, cyberbullying, and data breaches

The school delivers a planned online safety curriculum and provides ongoing staff training.

10. Review and Oversight

This policy will be reviewed annually or following significant technological or statutory changes.

Monitoring responsibility:

- Headteacher – strategic oversight
- Online Safety Lead/ICT Coordinator – operational monitoring
- Governing Body – compliance and challenge