Online Safety Policy

Policy Author	Tim Beavan
Date Ratified	February 2026
Ratified by	Full Governing Board
Statutory	No - Helps fulfil *statutory safeguarding expectations*
On school website	Yes
Main updates since last policy	Updated filtering/monitoring, added AI safeguards, strengthened parental guidance on devices and social media

1. Introduction

This policy explains how Wessex Primary School protects pupils, staff and families when using technology and the internet. It reflects our values of Honesty, Positivity, Respect and Pride and aligns with safeguarding and data-protection expectations. Online safety is a core part of safeguarding and is treated with the same rigour as all other safeguarding responsibilities.

2. Scope

This policy applies to all staff, pupils, volunteers, governors, visitors and community users. It covers the use of:

- school devices such as iPads, Chromebooks, computers and any other technology
- personal devices when on the school site
- school networks, filtering systems and Wi-Fi
- online tools and digital services used by the school
  It sits alongside the school's wider safeguarding framework.

3. Roles and responsibilities

Headteacher: Tim Beavan
Overall responsibility for online safety, ensuring policies and practices meet statutory safeguarding expectations and that staff understand their responsibilities.

Designated Safeguarding Lead (DSL): Anne Leigh
Lead responsibility for safeguarding including online safety, reviewing filtering and monitoring reports, responding to incidents and supporting staff and pupils.

Deputy DSLs: Tim Beavan, Sarah Pope, Hannah Denning
Support the DSL with online-safety responsibilities and act when the DSL is unavailable. Computing Lead: **Tim Beavan**
Oversees the online-safety curriculum, supports staff and works with the DSL on filtering and monitoring.

Technical provider: Agile ICT
Manages Fortinet filtering and monitoring, maintains appropriate security measures, provides weekly monitoring reports and supports the annual review.

Online Safety Governor: Naomi Churchill
Provides governance oversight, meets the DSL termly and monitors filtering and monitoring. All staff share responsibility for maintaining safe, responsible and lawful use of technology in line with safeguarding expectations.

4. Filtering and monitoring

The school uses Fortinet filtering, managed by Agile ICT.

Filtering:

- applies on all devices using school internet
- blocks illegal and harmful content
- provides differentiated filtering for staff and pupils
- is checked through formal filtering review processes

Monitoring:

- weekly reports are reviewed by the DSL and Computing Lead
- real-time supervision by staff acts as in-class monitoring
- CPOMS is used to log any online-safety concerns

An annual review of filtering and monitoring takes place with DSL, SLT, the Online Safety Governor and Agile ICT, with additional termly checks.

5. Curriculum

Online safety is taught through Computing, PSHE (Jigsaw), assemblies and pastoral support. Pupils learn about safe and respectful communication, privacy, passwords and personal information, recognising risks, evaluating online content, reporting concerns and healthy digital habits.

5.1 Online safety in Jigsaw PSHE

Jigsaw provides sequenced, age-appropriate teaching on managing online friendships, recognising pressure or inappropriate contact, understanding the impact of screen time and social media on wellbeing, dealing with cyberbullying, knowing how and when to seek help and making safe choices about sharing information. These messages are revisited and build over time. This reinforces the Computing curriculum and promotes our school values.

6. Mobile phones and devices

The school strongly discourages primary-aged children from owning mobile phones. Only Year 5 and 6 may bring mobile phones to school. Phones and network-enabled smartwatches must be switched off at the gate and handed to the class teacher. Fitness trackers without cameras, network access or internet connectivity are allowed. Where families choose for their child to own a phone, we ask for parental support in managing this responsibly. Personal devices must not be used for taking photos of pupils.

The school takes no responsibility for mobile phones or smart devices brought in to school by children.

7. Artificial Intelligence (AI)

Pupils must not use AI tools in school. Staff may use school-approved AI tools but must not enter identifiable or sensitive pupil data, must check accuracy and appropriateness of outputs and must ensure AI is used safely and professionally. Any new AI tool requires a Data Protection Impact Assessment before approval.

8. Incident reporting and response

All online-safety concerns are logged on CPOMS. The DSL assesses each concern and determines next steps. Serious or illegal issues may be escalated to police, the Local Authority Designated Officer or Children's Social Care. Parents are informed where appropriate, unless doing so places a child at risk. The school follows its safeguarding escalation routes.

9. Education for parents and carers

Parents and carers are supported through newsletters, website guidance, workshops, Safer Internet Day content and guidance on smartphone and social-media use for children.

10. Social media expectations

Staff follow the Staff Code of Conduct and use school systems for professional communication. Staff maintain professional conduct online and avoid posting content that could damage the school's reputation. Parents and carers should raise concerns directly with school, avoid posting negative or harmful comments about school matters online and keep event photos private rather than posting publicly.

11. Acceptable Use Agreements

The following Acceptable Use Agreements accompany this policy as appendices:

- EYFS and KS1
- KS2
- Staff
- Parents and Carers
- Community Users

These set out expectations for safe, responsible and respectful use of technology.

12. Review schedule

This policy will be reviewed every two years or sooner if required. The next review is due January 2028.

AUA 1: EYFS & KS1 – Our Technology Rules

When I use school devices such as iPads, Chromebooks, computers and any other technology, I will:

- listen to my teacher
- keep passwords private
- use only apps and websites my teacher says are safe
- not share my name, address or photos without asking an adult
- tell an adult if something worries me online
- be kind when I use technology
- look after the devices
- only use other people's work or pictures if a grown-up says I can
- take breaks from screens when my teacher asks me to

I know that adults in school can see what I am doing on school devices to help keep me safe.
I know that if I forget these rules, a grown-up will help me learn how to use technology safely.

AUA 2: KS2 – Using Technology Safely

When I use school devices such as iPads, Chromebooks, computers and any other technology, I will:

- keep my passwords private
- use only the apps and websites I am allowed to use
- not share personal information about myself or anyone else
- only talk to people I know in real life
- tell an adult if something online worries or confuses me
- be kind, respectful and responsible in messages and comments
- check information carefully before believing or sharing it
- ask before using someone else's work or images
- look after devices and report any damage
- never try to get around filtering, monitoring or security
- not use AI tools in school
- hand in my phone or smartwatch if I bring one
- make safe, sensible choices online and offline

I understand that the school can check what I do on school devices and systems to help keep everyone safe.
I understand that I must not have social media accounts such as TikTok, Instagram or Snapchat.

AUA 3: Staff – Professional Use

As a member of staff, I will:

- use school devices, accounts and systems responsibly and professionally
- keep passwords and access secure
- only use school-approved tools, including AI tools
- not enter personal or sensitive pupil data into unapproved tools

- communicate with families only through school systems
- maintain professional behaviour online
- avoid posting anything that could damage the school's reputation
- supervise pupils when using devices
- report online-safety concerns promptly
- not bypass filtering, monitoring or security controls
- follow the Code of Conduct when taking, storing or using images
- understand that network activity may be monitored for safety, safeguarding and operational reasons

  I understand my responsibilities under safeguarding, data protection and acceptable-use expectations.

AUA 4: Parents and Carers – Expectations

As a parent or carer, I understand that:

- the school uses filtering, monitoring and supervision to help keep children safe
- only Year 5 and 6 may bring phones to school, and these must be switched off and handed in
- fitness trackers without cameras or internet are allowed
- I may take photos of my own child at events but will keep them private and not post them publicly
- I will raise concerns directly with the school, not online
- I will model respectful online behaviour
- I will support my child to follow their AUA
- the school strongly discourages primary-aged children from owning mobile phones, and if our family chooses this, I will supervise my child's use

  I understand that the school may check use of its systems and networks to help keep pupils safe. I will work with the school to promote safe, responsible and respectful online behaviour.

AUA 5: Community Users – Responsible Use

When using the school's Wi-Fi, devices or systems, I will:

- use them responsibly for the agreed purpose
- keep the guest Wi-Fi password private
- not access or share inappropriate or illegal material
- not bypass filtering or security systems
- only take or share photos with staff permission
- report concerns to staff immediately
- use personal devices in line with school rules
- use any restricted login only as intended and never share it

  I understand that the school may monitor the use of its systems, Wi-Fi and devices to ensure safety and appropriate use and may restrict or remove access if expectations are not followed.