Bring your own device policy

Earley Springs

Written by	**Harriet Carter**	**September 2025**
Reviewed on		

Introduction

At Earley Springs we recognise that technology, when used responsibly, can support teaching, learning and communication. Increasingly, staff and visitors may wish to use their own personal devices such as laptops, tablets, or smartphones within the school. This policy sets out the expectations and safeguards around Bring Your Own Device (BYOD) to ensure that such use protects pupils, staff and the wider school community.

This policy must be read alongside the Earley Springs Child Protection and Safeguarding Policy, Online Safety Policy, Mobile and Smart Technology Policy, Acceptable Use Policy, Staff Code of Conduct and Keeping Children Safe in Education (KCSIE). Safeguarding principles apply at all times when personal devices are used on school premises.

Purpose

The purpose of this policy is to allow the responsible use of personal devices while safeguarding the security of school systems, the confidentiality of pupil information, and the wellbeing of children and young people. It aims to strike a balance between enabling flexible working practices and ensuring compliance with safeguarding, GDPR and data protection obligations.

Scope

This policy applies to all staff, volunteers, contractors, and visitors who wish to connect a personal device to the Earley Springs network or use their device on school premises. For safeguarding reasons, pupils are not permitted to bring their own devices unless this has been expressly agreed as part of an individual plan, for example through an EHCP or communication aid arrangement.

Safeguarding and Appropriate Use

The safety of our pupils is paramount. Staff must never use their own devices to take photographs, videos, or audio recordings of pupils. All such media must only be captured on school-owned devices, in line with our Safeguarding and Acceptable Use of ICT Policies. Any breach of this rule will be treated as a serious safeguarding matter.

Earley Springs recognises that many pupils have communication and interaction differences, sensory needs, or vulnerabilities which may increase their risk of online harm. Staff must take particular care to ensure that their use of personal devices does not expose pupils to risk, and must report any concerns immediately to the DSL.

Personal devices must not be used to store or transfer pupil information unless they are encrypted and access has been formally approved by the Headteacher. Where access is granted, staff must ensure that devices are password-protected, have up-to-date security software, and that school data is stored securely and not shared with unauthorised individuals.

The Designated Safeguarding Lead (DSL) will oversee any safeguarding concerns arising from the use of personal devices, including access to inappropriate content, data breaches, or concerns that device use may place a child at risk. All staff, volunteers, and visitors must follow the DSL's guidance in managing any safeguarding risks.

Access to the School Network

Staff and visitors may connect their devices to the school's designated guest Wi-Fi. This network is filtered and monitored in line with statutory safeguarding guidance. Direct access to the school's secure network is restricted to school-owned devices only. The use of personal data hotspots is discouraged during the school day to ensure consistent safeguarding monitoring.

Earley Springs meets the DfE Filtering and Monitoring Standards (2023). Personal devices connected to school Wi-Fi remain subject to filtering and monitoring to ensure compliance with safeguarding legislation. Staff and visitors must not use mobile hotspots or unfiltered networks to bypass safeguarding systems.

Data Protection

All users of personal devices must comply with UK GDPR and the Data Protection Act 2018. Pupil records, reports and sensitive information should only be accessed through secure, school-approved platforms and never downloaded or stored locally on a personal device. In the event of a lost or stolen device containing school data, this must be reported to the Headteacher and Data Protection Officer immediately.

Responsibility and Liability

The school accepts no responsibility for the maintenance, repair, loss or theft of personal devices brought onto site. All users remain responsible for their own property. Staff and visitors are advised to ensure their devices are insured and appropriately protected.

Monitoring and Compliance

Earley Springs reserves the right to monitor the use of personal devices on school premises or when connected to the school network to ensure compliance with safeguarding and data protection standards. Any misuse of personal devices, including attempts to access inappropriate material or breach confidentiality, will be treated seriously and may result in disciplinary action or withdrawal of access.

Any breach of this policy, including conduct that may amount to a low-level concern or behaviour inconsistent with safer working practice, must be reported to the Headteacher or DSL in line with KCSIE Part 4. Personal device misuse may constitute a safeguarding concern and will always be treated seriously.

Review of Policy

This policy will be reviewed annually, or sooner if required in light of changes to legislation, safeguarding guidance, or school procedures.