Lawford CE Primary School

Bring Your Own Device (BYOD) Policy

Ratified by FGB – 20th March 2019

Reviewed 10th March 2026

Annual review

Updates since last policy:
MFA added to use of official app.

Bring Your Own Device (BYOD) Policy

Introduction

1. Lawford C of E Primary School recognises that mobile technology offers valuable benefits to staff from a teaching and learning perspective and to visitors. Our school embraces such technology but requires that it is used in a safe and responsible way.

2. This policy is to address the use by staff members/ visitors and pupils of non-school owned electronic devices connecting to the internet either via school WiFi or through the use of mobile data. The term mobile devices includes (but the list is not exhaustive) smart phones, tablets, laptops, wearable technology – if you are unsure you should ask at Reception. This policy complements, and should be read in conjunction with, our 'Acceptable Use' documents in the 'online safety' policy and 'staff code of conduct'.

Use

3. Typically, staff must only use their personal mobile devices in the staff room or offices during the school day. Once the children have left for the day they may also be used in classrooms. Staff needing a device to monitor a medical condition may use them in class to monitor their condition as needed and staff may use them where two factor authentication is required using a mobile deice to access software approved by the school – e.g. Insight or Microsoft. The device should then be put away and silent. By exception, they may also be used as part of planned lessons with prior agreement of the Headteacher. Visitors to the school may use their devices in the school environs but not in the classroom. Staff and visitors are responsible for their devices at all times.

4. Pupils may bring mobile devices in to school if they are required for communication/security to and from school. Devices should be handed in to the school office once on site and retrieved at the end of the school day. The devices should be clearly labelled with the child's name and class. If a device is found by a member of staff not to have been handed in, then it will be confiscated and taken to the school office. It will be returned to a responsible adult at the end of the day.

5. Some children may be given permission to bring in mobile devices as a support to their learning/health. This will be agreed both with the SENCo and/or Head teacher. Examples of such permission may include the use of e- readers so that font size and colour can be changed, or if children have specific apps needed to monitor a health condition.

6. The school is not responsible for the loss, theft of, or damage to the device (incl. any removable storage) howsoever caused. Should such incidents occur please notify Reception and the incidents will be logged. Mobile devices must be turned off when in a prohibited area/at a prohibited time. They must not be taken into controlled examinations/assessments unless special circumstances apply. The school reserves the right to refuse staff and visitors permission to use their devices on school premises.

Access to the School's internet connection

7. The school permits staff and pupils (where permission for use of their own devices has been granted) access to its wireless network to allow internet use. Visitors and governors may use the 'Lawford Guest' Wi-Fi at the Headteacher' s discretion. This permission is at the discretion of the school and may be withdrawn if in the school's opinion it has been used inappropriately. The school advises against downloading any apps using the school's Wi-Fi. Parents should ensure that if the school has granted permission for a child to access the network to support their learning in school, they remind their children not to download apps or other files /file extensions in school. The school cannot guarantee despite high levels of filtering and monitoring that the access is secure and staff (visitors/pupils) use it at their own risk. The school accepts no liability for any loss of data or damage to the owner's device as a consequence of use of the school's wireless network.

Access to School IT services

8. Staff are permitted to connect to or access the following school IT services from their mobile devices:

    a. The school email system (where any relevant encryption technologies have been deployed).
    b. Their school 'One Drive' accessible through their Office 365 account as long as this does not hold personal data.
    c. Official School Apps including - MFA
    d. Staff are only allowed to use IT systems and information accessed for work purposes.

9. School information accessed through these services is confidential. Staff must take all reasonable steps to prevent unauthorised access to it. If it is necessary to open email attachments on the device which contain personal data (these documents must be password protected) they must be deleted once read. They are not to be stored on a personal device. Any security breech must be reported immediately to the Headteacher and they will act in line with our Data Protection Policy and Privacy Notices. Staff must not send school information (including planning) to their personal email accounts. Staff must report the loss of any device that contains school information. All personnel must ensure that no school information is left on any personal device indefinitely. Particular care must be taken if the device is disposed of/sold/transferred to a third party.

Security of personal devices

10. All personnel with permission to use their devices in school must take all reasonable steps to prevent unauthorised access to their devices, including, but not limited to, the use of a PIN, pattern, biometrics, or password to be entered to unlock the device and by ensuring that the device auto-locks if in active for a short period of time. All personnel are reminded to familiarise themselves with the school's online-safety and acceptable use policies. Anyone with permission to use their device in school must not try and bypass any security controls or in school systems or other devices. All personnel must ensure that their devices have appropriate security software installed and the must ensure that the software and security settings are up to date. Passwords must be kept securely and not be accessible to third parties.

Use of cameras and audio recording equipment

11. Parents and Carers may take photographs, videos or audio recordings of their children at school events for their own personal use. Staff may only use school equipment to take photos, videos

or audio recordings of children. Photos, videos or audio recordings must not be published on blogs, social networking sites (apps) or in any other way without the permission of the people identifiable in them (completed by parents for children annually). Devices must not be used to record people at a time when they would not expect to be recorded and devices must not be used that would allow a third party acting remotely to take photographs, video or audio recording in school.

Monitoring the use of personal devices

12. The school may use technology that detects and monitors the use of personal and other electronic or communication devices which are connected to or logged on to the school's wireless network or IT systems. By using a device on the school's network, staff and visitors agree to such detection and monitoring. The school's use of such technology is for the purpose of ensuring the security of its IT systems and tracking school information. The information that the school may monitor includes, (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms, information uploaded or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

13. Staff who receive any inappropriate content through school IT services or the school internet connection should report this to the school as soon as possible.

Support

14. The school takes no responsibility for supporting staff's own devices, nor does the school have a responsibility for conducting annual PAT testing of personal devices. However, the school will support staff in ensuring that they have appropriate levels of security in place.

Compliance, sanctions and disciplinary matters for staff

15. Non-compliance of this policy exposes both staff and the school to risks. If a breach of this policy occurs, staff may be subject to disciplinary action in line with the Code of Conduct.