



Use of Mobile Technologies Policy

River Bank Primary School

2026

1.0 Purpose:

The term 'mobile technologies' describes smartphones, tablets, notebooks / laptops or other technology owned or provided by the school, or privately owned, that can connect to the school's wireless network. This connection enables access to the wider internet including the school's learning platform and other services such as email and data storage.

When considering the use of mobile technologies all staff and the wider school community must understand that the primary purpose of having their personal device at school is educational and is irrespective of whether the device is school owned/provided or personally owned.

This policy should complement and be referenced in a range of policies including but not limited to the Safeguarding Policy, Acceptable Use Policy, policies around theft or malicious damage and the Behaviour Policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

2.0 Considerations:

Our school policy prohibits the use of mobile phones throughout the school day for pupils in all circumstances. They should not be brought in to school.

<https://www.gov.uk/government/publications/mobile-phones-in-schools/mobile-phones-in-schools>

There are a number of issues and risks to consider around the use of mobile devices in school for **adults**. These include:

- security risks in allowing connections to your school network.
- filtering of personal devices.
- breakages and insurance.
- access to devices for all students.
- potential classroom distraction.
- network connection speeds.
- cost to the school.

The school Acceptable Use Agreements for staff will include the use of mobile technologies.

The school allows:

	School Devices			Personal Devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device (purchased by the family through a school-organised scheme)	Pupil/Student owned	Staff owned	Visitor owned

Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet	Yes	Yes	Yes	No	Yes (Guest Wi-Fi)	Yes (Guest Wi-Fi)

Our school provides technical solutions for the safe use of mobile technology for school devices/personal devices:

- All iPads and Chromebook devices are controlled through the use of Mobile Device Management (MDM) software.
- Appropriate access control is applied to all mobile devices according to the requirements of the user.
- We have ensured that core educational and administrative activities are not negatively affected by the increase in the number of connected devices.
- Filtering will be applied to the internet connection for all devices.
- An authorised user will implement appropriate exit processes for devices no longer used at a school location. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licensed software etc.
- All school devices are subject to routine monitoring.
- Pro-active monitoring has been implemented to monitor activity.

3.0 Where personal devices are permitted:

- All personal devices are restricted to provide appropriate levels of access e.g. TEAMS, Arbor.
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school.
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover out of home use).
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. All devices should have their locking system enabled.
- The school is not responsible for the day-to-day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

3.1 Staff users are expected to act in line with Acceptable Use Agreements. When using personal or school owned devices, staff should be aware that:

- They are responsible for keeping their device up to date through software, security and app updates. The device should be virus protected and should not be capable of passing on infections to the network.
- They are responsible for charging their device and for looking after it while in school.
- Personal devices should be charged before being brought to school, charging of personal devices is permitted during the school day however the plug must be PAT tested.
- Devices must be in silent mode on the school site while in non-staff areas. The staff member's mobile phone is permitted for use during off-site activities for contacting the school, colleagues and relevant authorities during emergencies.
- Confiscation and searching - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The changing of settings on a school owned device (exceptions include personal settings such as font size, brightness, etc...) that would stop it working as it was originally set up is not permitted.
- The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of school owned devices will be made to ensure that users have not removed required apps.
- They should be aware of the age restrictions on apps and should read the terms and conditions before use.

4.0 Multi Factor Authentication:

Staff owned devices should not be used for personal purposes during teaching sessions, apart from for multi factor authentication.

Use of a mobile phone is permitted for multi factor authentication with River Bank Accounts. This should only be completed discretely with an awareness of where pupils are in the room.

When logging into a cover laptop or TA laptop, please make sure you login into office 365 before leaving the staff room or office.

For all devices that require access to Outlook, TEAMS, Arbor and Insight, you will have to authenticate regularly. Every time you login into a new or different device you will be required to authenticate.

When staff purchase a new phone, it is their responsibility to inform the IT Team so that multi factor authentication can be set up on the new device preventing loss of account access.

5.0 Parent, Visitors or Volunteers in School Policy:



- Adults either in school or accompanying children on school trips should not use their personal cameras or mobile phone cameras to take pictures of pupils unless it is at a public event such as sports day or summer fair and of their own children.
- Adults, visitors or volunteers in school should only use their mobile phone within the confines of the school office, staff room and spaces where no children are present. Personal cameras and mobile phone cameras should not be used to take pictures of children. If parents who accompany children on a school trip are asked by the teacher to take photos as a record of the educational visit, they will be issued with a school camera or school phone. Parents accompanying children on school trips should not use their mobile cameras to take pictures of children.

6.0 Staff policy

Staff use of mobile phones for personal reasons during their working day should be:

- outside of their contracted hours
- discreet and appropriate e.g. not in the presence of pupils (including all premises staff).
- Mobile phones should be switched off and left in a safe place during lesson times. The school cannot take responsibility for items that are lost or stolen.
- Staff should avoid contacting pupils or parents from their personal mobile phone or give their mobile phone number to pupils or parents. If a member of staff needs to make telephone contact with a pupil, they should use the school telephones or withhold their number.
- Staff should never send to, or accept from, colleagues or pupils, texts or images that could be viewed as inappropriate.
- With regard to camera phones, a member of staff should avoid using their phone to photograph a pupil(s) or allow themselves to be photographed by pupils. There may be a circumstance e.g. residential, where colleagues may use their own devices and share images with the group leader who will then supervise deletion.
- Mobile Phones can be taken outside when teaching PE
- Parent meetings can take place over personal mobile phones if the staff member withholds their number.

This guidance should be seen as a safeguard for members of staff and the school. Staff should understand that failure to comply with the policy is likely to result in the enforcement of the Whistleblowing policy and associated procedures.

7.0 Insurance:

You should consider how you will insure school devices owned under your household insurance

8.0 Use of school Trip Phone

8.1 Purpose:

This section aims to set the guidelines and acceptable use of the school trip phone(s).

8.2 Scope:

The policy covers any staff member who use the trip phone(s) for any trip or purpose deemed appropriate.

8.3 Policy Statements:

The phone is permitted only to be used during the school trip and must not be used for any other purpose other than for River Bank trips unless permission is provided by the headteacher.

The staff member is fully responsible for the phone while on the trip. Any damage to the device should be reported to the headteacher and IT team. If the device is lost or stolen, there should be no delay in communicating this to the school so the required action(s) can be taken.

8.4 The numbers are as followed:

07506 031835

07506 039537

8.5 The phone should only be used for the following:

- Photos and permission: Take photos of the trip for use on class DOJO. Staff members are permitted to use the trip mobile phones during school trips as part of their duties.
- Staff can send the photos using WhatsApp to the school's IT Team for posting to the class DOJO. Please include a description of the photo/ trip you wish to be added to the post.
- Staff can also upload photo to Teams using the pre-logged in account.
- Educational and Administrative Use: Mobile phones should be used for educational purposes, such as coordinating activities, researching relevant information, and communicating with other staff members.
- Safety and Emergency: Mobile phones may be used for contacting emergency services, school administration, or parents/carers if necessary.
- The school number, IT Network manager number, Family worker number and the other trip phone will be listed as a contact on the device. All other emergency numbers should follow the schools normal trip procedure.
- Prohibited Use: Mobile phones should not be used for personal activities such as social media, personal calls, or streaming videos This includes but is not limited to, X, Facebook and WhatsApp. Staff must also not search any material other than what is required for the trip. – The school's trip phone is strictly for work use only.
- Respect and Privacy: Staff members must respect the privacy of others. Unauthorized photos, videos, or audio recordings of students, staff, or third parties are strictly prohibited.
- Data Security: Users should not download or install unauthorized apps on the shared mobile phone. Any data or information stored in the phone should be treated as confidential. App installs are only to be carried out by the school's IT team.
- Physical Security: The shared mobile phone(s) should be kept in a secure place when not in use. The phone(s) will also be secured by at least a 4-pin password.
- Usage Log: Users should maintain a log of their usage including date, time, and purpose of use. The device needs to be signed in/out using the appropriate form. Use of the phone can only be approved by the headteacher. The form can be found at the end of this policy.
- Cleanliness: Users are responsible for keeping the shared mobile phone clean and sanitized upon returning the device. The Phone must also remain in the provided case at all times.

- The user should ensure that the battery is charged to 100% before leaving site for the trip. If the trip is longer than one day, the user will need to ensure they have taken the allocated charger.

8.6 Training and Awareness:

Staff should refer to the Security Awareness and Training Policy for training. Regular training will be provided to all staff at the school. Staff must,

- Attend mandatory security training sessions to stay informed about best practices.
- Familiarize yourself with our acceptable use and mobile phone policy and adhere to its guidelines.

Staff members will be trained upon appointment and will receive updates/ re-training annually

8.7 Enforcement:

Non-compliance with this policy may result in disciplinary action, including but not limited to retraining, suspension, termination, or legal action, depending on the severity and recurrence of the violation.

8.8 Revision History:

This policy will be periodically reviewed and updated as needed to reflect changes in technology, business requirements, and regulatory obligations. Any revisions to the policy will be documented with a clear record of changes and their rationale

8.9 Acknowledgment:

All employees, contractors, and third-party vendors are required to acknowledge their understanding and acceptance of this policy.

9.0 Sign out/ in form for trip phones – Please see next page:

Signed: 

Adopted: September 2026

Review Date: September 2027



[illegible]

Please print off this document and read it carefully.

By signing this form, you agree that you have been provided with a copy of the School's Use of Mobile Technologies Policy and that you have read and understood the policy. The policy forms part of your terms and conditions of employment with the School.

Signed

Printed Name

Position.....

Date.....

Signed forms should be returned to:

Kieran Kitchener

