St Edmund's Catholic Primary School

&

St Joseph's Catholic Primary School

OWN DEVICE POLICY

Policy Adopted: Summer 2018

Reviewed: Summer 2023

Review Date: Summer 2025

Contents

Bring Your Own Device Policy

Part 1 Introduction

St Edmund's and St Joseph's Catholic Primary Schools recognise the benefits of mobile technology and are committed to supporting staff in the acceptable use of mobile devices.

This policy describes how non-school owned electronic devices, e.g. laptops, smart phones and tablets, may be used by staff members and visitors to the schools. These devices are referred to as 'personal devices' in this policy. If you are unsure whether your device is covered by this policy, please check with the Data Protection Officer.

Part 2 Organisational Arrangements

Overall Responsibility

The Governing Body of the schools is responsible for the approval of this policy and for reviewing its effectiveness.

Roles & Responsibilities

Where it has been agreed that a member of staff may use their own device (see 'access to schools' systems) staff members will:

- Familiarise themselves with their device and its security features so that they can ensure the safety of school information.
- Install relevant security features and maintain the device appropriately.
- Set up passwords, passcodes, passkeys or biometric equivalents on the device being used.
- Set up remote wipe facilities if available, and implement a remote wipe if they lose the device.
- Encrypt documents or devices as necessary.
- Report the loss of any device containing school information, or any security breach immediately to the Data Protection Officer.
- Ensure that no school information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of / sold / transferred to a third party.

Visitors will:

- Familiarise themselves with the use of personal devices at the school.
- Only use personal devices for agreed purposes at the school and with parental or the relevant permission.
- Not share information from personal devices via social media and will not keep school information indefinitely.

Part 3 Detailed Arrangements & Procedures

Use of personal devices at the school

Other than phones, staff should not use their own devices in school. Staff should only use phones in areas of the school where children would not expect to be present eg staff room, offices.

Personal devices must be switched off when in a prohibited area, and / or at a prohibited time, and must not be taken into controlled assessments and / or examinations unless special circumstances apply.

The schools reserve the right to refuse staff and visitors permission to use their own device on school premises.

Use of cameras and audio recording equipment

Parents and carers may take photographs, videos or audio recordings of their children at school events for their own personal use when permission is given by a member of the Leadership Team.

Other visitors and staff may use their own personal devices to take photographs, video, or audio recordings in school provided they have checked that parental permission has been received by the school. This includes people who may be identifiable in the background.

Photographs, video or audio recordings made by staff on their own devices should be deleted as soon as reasonably possible after they have been used, e.g. uploaded for use on one of the schools' social media sites. Photographs, video or audio recordings to be retained for further legitimate use, should be stored securely on the school networks.

Photographs, video or audio recordings should not be published on blogs, social networking sites or in any other way without the permission of the people identifiable in them.

Devices must not be used to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video or audio recordings in school.

Access to the schools' systems

In order to increase data security, those members of staff who may routinely need to access school information eg emails outside the school buildings will be supplied with a school device. It is recognised however that there may be occasions where the use of a member of staff's own device may be necessary. In this event, staff are permitted to connect to or access the following school services from their device, ensuring they follow the guidance highlighted in 'roles and responsibilities' in part 2:

- The school email system.
- The school management information system.

Staff may use the systems to view school information via their personal devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their device. In some cases, it may be necessary for staff to download school information to their personal

devices in order to view it (e.g. an email attachment). Staff shall delete this information from their device as soon as they have finished viewing it.

Staff must only use the IT systems and any information accessed through them for work purposes. School information accessed through these services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to, or distribution of, confidential information should be reported to the school as soon as possible.

Staff must not send school information to their personal email accounts.

Monitoring the use of personal devices

The schools may use technology that detects and monitors the use of personal and other electronic or communication devices which are which are used to access school information such as email or are connected to or logged on to the schools' wireless network or IT systems. By using a device on the schools' network, staff and visitors agree to such detection and monitoring. The schools' use of such technology is for the purpose of ensuring the security of its IT systems and tracking school information.

The information that the schools 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.

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

Security of staff personal devices

Any member of staff given permission to use their own device must ensure that the device they choose to use has the benefit of encryption. This should be more than a simple password protection.

Staff must ensure that personal devices are set to lock with encrypted passcodes to prevent unauthorised access. The device should be locked if they are unattended or set to auto-lock if it is inactive for a period of time.

Staff must never attempt to bypass any security controls in school systems or others' own devices.

Staff must ensure that personal devices are configured to prevent other home users such as friends and family from accessing school data (for example by not allowing browsers to remember passwords or use apps that stay signed in etc.). Passwords must also be kept securely and not accessible to third parties.

Appropriate security software must be installed on their personal devices including firewall and anti-virus software, and must keep the software and security settings up-to-date.

Support

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

Compliance, sanctions and disciplinary matters for staff

Non-compliance of this policy exposes both staff and the schools to risks. If a breach of this policy occurs, the Staff Disciplinary policy will be applied.

Incidents and reporting

The schools take any security incident involving a staff member's or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of the device should be reported to the school office in the first instance. Data protection incidents should be reported immediately to the schools' Data Protection Officer.

The governor with responsibility for GDPR will monitor this policy and procedures annually. The IT subject leader and SBM will report annually to the Governing Body.