Bring Your Own Device Policy

Approved by:	CEO	Date: 25/04/2024
Reviewed by:	Head of School	
Last reviewed on:	21/05/2025	
Next review due by:	24/04/2026	

Contents

1.1 Introduction

- Releasing Potential recognises that mobile technology offers valuable benefits to the Company, staff and students from a teaching and learning perspective and to visitors. Our Company embraces this technology but requires that it is used in an acceptable and responsible way. Staff should not feel compelled to use their own personal devices to access Company systems, but if staff choose to use their own devices, this policy should be adhered to.

- This policy is designed to support the use of guest devices (any device which is not Organisation owned or on the Organisation asset list) in Company in a way that extends and enhances teaching and learning. It also aims to protect children from harm, minimise risk to the Company networks and explain what constitutes acceptable use and misuse of the BYOD policy.

- This policy supports our Data Protection Policy and provides guidance on how to minimise risks associated with the use of guest devices, in line with the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

- The Company reserves the right to refuse staff and visitors permission to use their personal devices on Organisation premises.

- This applies to all guest devices connecting to Company systems.

- This policy does not stand alone, it is essential to follow the requirements set out in the ICT & Internet and Online Safety Policies, which provides more details as well as guidance.

1.2 Scope and Responsibilities

This policy applies to all use of guest devices to access the internet via the Organisation network or to access Company information, by staff, pupils or visitors. This is known as "Bring Your Own Device," or "BYOD." Guest devices include laptops, tablets, smart phones, USB sticks, wearable technology (including smart / apple watches) and any other device considered portable and/or with the ability to connect to Wi-Fi and the Internet which is not Company owned or on the asset list, including staff personal devices.

All staff are responsible for reading, understanding and complying with this policy if they are using their personal devices connected to the Company's Internet, or using personal devices to access information held on Company systems.

If you have any concerns surrounding the use of personal devices, please contact a senior member of staff or a Designated Safeguarding Lead.

Users should be aware of the need to;

- Protect children from harm
- Understand what constitutes misuse
- Minimise risk from BYOD
- Report suspected misuse immediately
- Be responsible for their own professional behaviour
- Respect professional boundaries

1.3 Use of mobile devices

Permission must be sought before connecting personal devices to the Organisation's network. The Company reserves the right to refuse staff, pupils and visitors permission to use their personal devices on Company premises.

Staff, pupils and visitors are responsible for their personal devices at all times. Releasing Potential is not responsible for the loss, or theft of, or damage to the personal device or storage media on that device (e.g., removable memory card) howsoever caused, including lost or corrupted data.

The Company must be notified as soon as possible of any loss, or theft of a personal device that has been used to access Company systems, and these incidents will be logged with the DPO.

Data protection incidents should be reported immediately to the Data Protection Officer.

Personal devices used to access Company systems must enable automatic updates for security patches from the supplier. Applications installed on the device must also be subject to regular security updates, be supported by the supplier and licensed.

The Organisation cannot support users' personal devices, nor has the Company a responsibility for conducting annual PAT testing of personal devices.

1.4 Access to the Organisation Internet connection

The Company provides a network connection that staff, pupils and visitors may, with permission, use to connect their personal devices to the Internet. Access to the network is at the discretion of the Company, and the Company may withdraw access from anyone it considers is using the network inappropriately.

The Company cannot guarantee that the wireless network is secure, and staff, pupils and visitors use it at their own risk. In particular, staff, pupils and visitors are advised not to use the wireless network for online financial transactions.

With permission the Company permits the downloading of apps or other software whilst connected to the Company network. The Company is not responsible for the content of any downloads onto the user's own device whilst using the Company's network.

The Company accepts no liability for any loss of data or damage to personal devices resulting from use of the Company's network.

1.5 Access to Company IT systems

Where staff are permitted to connect to Company IT systems from their personal devices, a second layer of security should be enabled such as a password and/or encryption and notifications must be turned off the lock screen. It is the responsibility of the owner of that device to ensure it is safe for the purposes for which they wish to use it.

Staff must transfer personal data about pupils held on any non-company devices onto the Company's cloud based system and delete all student data stored on non-company devices.

On occasion , it may be necessary for staff to download Company information to their personal devices in order to view it (for example, to view an email attachment). Email attachments are the most common source of cyber-attacks. Please follow staff guidance on cyber security and email protection and be aware that personal devices are not subject to the same security controls and safeguards that protect the Company network and devices.

Any unauthorised access to, or distribution of, confidential information should be reported to a senior staff member and the Data Protection Officer as soon as possible in line with the Company's data protection policies. This includes theft or loss of a personal device which has been used to connect to Company information systems or which may contain personal data.

Before selling or giving your personal device which has been used to access the Company network including cloud-based systems to someone else, including a family member or spouse, it must be cleansed of all related data, emails, systems and apps.

1.6 Monitoring the use of mobile devices

The company reserves the right to use technology that detects and monitors the use of personal devices, which are connected to or logged on to our network or IT systems. The use of such technology is for the purpose of ensuring the security of its IT systems and company information.

The information that the company 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 to or downloaded from websites and company IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Any inappropriate content received through the company's IT services or internet connection should be reported to their line manager, Vox IT and if necessary a Designated Safeguarding Lead as soon as possible.

1.7 Security of staff personal devices

Staff must take all sensible measures to prevent unauthorised access to their personal devices, including but not limited to the use of a PIN, pattern or password to unlock the device, and ensuring that the device auto-locks if inactive for a short period of time.

The company's ICT, Internet and Online Safety policies set out in further detail the measures to ensure responsible behaviour online.

1.8 Permissible and non-permissible use

Staff and visitors participating in BYOD must comply with the ICT & Internet Policy.

1.9 Use of cameras and audio recording equipment

Visitors subject to this policy may not use their own mobile devices to take photographs, video, or audio recordings whilst on site, unless they have specific permission from the CEO.

In order to protect the privacy of our staff and pupils, and, in some cases their safety and wellbeing, photographs, video, or audio recordings must not be published on blogs, social networking sites or disseminated in any other way without the permission of the people identifiable in them.

No one must use mobile devices 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

Links to other policies: -

Staff code of conduct .docx

ICT & Internet Policy.docx

Online Safety Policy.docx

[Visitor and Contractor Policy.docx](Visitor%20and%20Contractor%20Policy.docx)

[Mobile Phones.docx](Mobile%20Phones.docx)