OLDFIELD SCHOOL

BRING YOUR OWN DEVICE POLICY

Last Review:	April 2023
Committee:	SLT
Date Ratified:	26/04/2023

1. Introduction

Oldfield School recognises that there are benefits that can be achieved by allowing staff to use their own electronic devices when working, whether that is at home, on site or while travelling. Such devices include laptops, smart phones and tablets, and the practice is commonly known as 'bring your own device' or BYOD. However, the use of such devices to create and process School information and data creates issues that need to be addressed, particularly in the area of information security.

The School must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering staff to ensure that they protect their own personal information.

2. Information security policies

2.1. All relevant School policies still apply to staff using BYOD. Staff should note, in particular, the School's Information Security related policies. Several of these are directly relevant to staff adopting BYOD:

- ICT policy
- Online safety Policy
- Freedom of Information Policy
- Code of Conduct for Staff

3. The Responsibility of Staff Members

3.1. Individuals who make use of BYOD must take responsibility for their own device and how they use it. They must:

- Familiarise themselves with their device and its security features so that they can ensure the safety of School information (as well as their own information);
- Invoke the relevant security features;
- Maintain the device themselves ensuring it is regularly patched and upgraded;
- Ensure that the device is not used for any purpose that would be at odds with the School's ICT Policies.

3.2. Staff using BYOD must take all reasonable steps to:

- Prevent theft and loss of data;
- Keep information confidential where appropriate;
- Maintain the integrity of data and information, including that on site;
- Take responsibility for any software they download onto their device.
- Partition any school data in a separate folder and password protect that folder.

3.3. Staff using BYOD must:

- Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device;
- Set up remote wipe facilities if available and implement a remote wipe if they lose the device;
- Encrypt documents or devices where possible;
- Not hold any information that is related to safeguarding, HR, finance or any data that may pose a high risk to data subjects;
- Where it is essential that information belonging to the School is held on a personal device it should be deleted as soon as possible once it is no longer required. This includes information contained within emails;
- Report the loss of any device containing School data (including email) to the IT Help desk;
- Be aware of any data protection issues and ensure personal data is handled appropriately;
- Report any security breach immediately to the IT Helpdesk in accordance with the Data Protection Breach policy);
- 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.
- Ensure that data created on personal devices is copied to school databases as soon as practicable. (to avoid data inaccuracy).
- Not use cloud backups to copy any data to another location beyond the personal device.
- Not use any school data held, for any purpose other than that which has been specified by the school and defined in the Privacy Notice provided to students, parents or staff.

3.4 Staff accessing SIMS Connected on a personal device:

- Complete the form forwarded from the network manager requesting permission to do so;
- Wait until authorised before accessing SIMS Connected on their personal device.

4. Monitoring and Access

4.1. The School will not routinely monitor personal devices. However, it does reserve the right to:

- Prevent access to a particular device from either the wired or wireless networks or both;
- Prevent access to a particular system;
- Take all necessary and appropriate steps to retrieve information owned by the School.
- Clarify verbally what data is held on the device.
- Provide any data that is subject to a Freedom of Information Act or Subject Access Request.

5. Data Protection and BYOD

5.1. The School must process 'personal data' i.e. data about identifiable living individuals in accordance with the Data Protection Act2018. Sensitive personal data is information that relates to race/ethnic origin, political opinions, religious beliefs, trade union membership, health (mental or physical) or details of criminal offences. This category of information should be handled with a higher degree of protection at all times.

5.2. The School, in line with guidance from the Information Commissioner's Office on BYOD, recognises that there are inherent risks in using personal devices to hold personal data. Therefore, staff must follow the guidance in this document when considering using BYOD to process personal data.

5.3. A breach of the Data Protection Act can lead to the School being fined. Any member of staff found to have deliberately breached the Act may be subject to disciplinary measures, and be personally liable for any financial penalty incurred as a result of a data breach, having access to the School's facilities being withdrawn, or even a criminal prosecution.