Bring Your Own Device ("BYOD") Policy

This policy applies to the whole school

Introduction

The School recognises the benefits that can be achieved by allowing staff to use their own electronic devices when working, whether that is at home, at School or while travelling. Such devices include laptops, smart phones and tablets, and the practice is commonly known as 'bring your own device' or BYOD. The School is committed to supporting staff in this practice and ensuring that as few technical restrictions as reasonably possible are imposed on accessing School provided services on BYOD.

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.

The school has outsourced its IT services and support to Stone. For the purposes of this policy Stone staff will be referred to as IT Staff or IT helpdesk (service.desk@jagsit.freshdesk.com).

Information Security Policies

All relevant School policies still apply to staff using BYOD. Staff should note the Online Safety policy.

The Responsibilities of Staff Members

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

Owner: Director of Operations
Bring Your Own Device Policy Reviewed December 2023
Next Review: January 2025

- 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 Online Safety and the School Code of Conduct.

While IT staff will always endeavour to assist colleagues wherever possible, the School cannot take responsibility for supporting devices it does not provide. 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
- Take responsibility for any software they download onto their device

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 as necessary
- Not hold any information that is sensitive, personal, confidential or of commercial value on personally owned devices. Instead they should use their device to make use of the many services that the School offers allowing access to information on School services securely over the internet.
- 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
- Ensure that relevant information is copied back onto School systems and manage any potential data integrity issues with existing information
- Report the loss of any device containing School data (including email) to the IT Help desk and the Director of Operations.
- Be aware of any Data Protection issues and ensure personal data is handled appropriately.
- Report any security breach immediately to IT Helpdesk in accordance with the Data Breach Response Plan
- 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

Monitoring and Access

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

- Prevent access to a particular device from either the wireless networks
- Prevent access to a particular system
- Take all necessary and appropriate steps to retrieve information owned by the School

Data Protection and BYOD

The School must process 'personal data' i.e. data about identifiable living individuals in accordance with the Data Protection Act 2018. Sensitive personal data is information that relates to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. This category of information should be handled with a higher degree of protection at all times. 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.

A breach of the Data Protection Act can lead to the School being fined up to £9 million, or 2% annual turnover, whichever is higher. Any member of staff found to have deliberately breached the Act may be subject to disciplinary measures, having access to the School's facilities being withdrawn, or even a criminal prosecution.

Information to Help Staff

The School has implemented a remote access solution to provide a remote access service for staff and pupils. Access instructions can be found here:

R:\Handbooks, guides & forms\IT Help Guides\INFO - Remote Access

The School has also provided a JAGS Intranet page via SharePoint to access online services such as curriculum applications and shortcuts to your files. Access Instructions can be found here:

R:\Handbooks, guides & forms\IT Help Guides\INFO - Accessing Your Email Online.pdf

BYOD is limited to the WiFi Network via JAGS BYOD. Please use your normal school credentials to login.