# Bring Your Own Device Policy (Staff)

| **Document Control Box** | |
|---|---|
| **Document title** (include version number if amended within same year as approved) | **Bring Your Own Device Policy (Staff)** |
| **Reference Number** | 008/22 |
| **Approval category (Please indicate)** | |
| Governance/Governor | **X** |
| MPRIG Executive/Other Committee (insert name) | |
| Senior Staff (insert name) | |
| **Date document approved** | 7/4/22 |
| **Supersedes** (insert previous title and/or version date) | N/A |
| **Date document last reviewed and/or updated** | |
| **Date next due for review** | January 2025 |
| **Related statutes or regulations** | |
| **Related policies/procedures/guidance/forms** | • Data Protection Policy<br>• Data Breach Procedure<br>• Information Communications Technology Acceptable Usage Policy<br>• Information Communications Technology Guidelines for Staff and Volunteers<br>• Social Media Guidelines for Students and Staff |
| **Staff member responsible for update** | Head of Services |

**Amendment History**

| Version | Revision Summary | Date Approved | Author |
|---|---|---|---|
| | | | |

# Bring Your Own Device Policy (Staff)

## Introduction

1. Spurgeon's College recognises the benefits that can be achieved by allowing staff to use their own electronic devices when working, whether at home, in College 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 College is committed to supporting staff in this practice and to ensuring that as few technical restrictions as reasonably possible are imposed. However, the College must also maintain the security of its systems and data at all times.

2. The College 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.

## Scope

3. This policy applies to all contracted staff and any volunteers, who use or have access to College data (electronic), systems or information.

## Information Security Policies

4. All relevant policies apply to staff using BYOD. Staff should ensure that they familiarise themselves with these policies and their contents.

   Data Protection Policy

   Data Breach Procedure

   Information Communications Technology Acceptable Usage Policy

   Information Communications Technology Guidelines for Staff and Volunteers

   Social Media Guidelines for Students and Staff

## The Responsibilities of Staff Members

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

a. Familiarise themselves with their device and its security features so that they can ensure the safety of College information (as well as their own information)
b. Activate the relevant security features on their devices
c. Maintain the device themselves ensuring that it is upgraded as necessary and safe to use in conjunction with College equipment
d. Ensure that the device is not used for any purpose that would be contrary to College policies, guidelines or values
e. While the IT Department will always endeavour to assist colleagues where possible, the College cannot take responsibility for supporting personal devices
f. Ensure that the device is adequately insured as necessary. Personal devices are not covered by the College's insurance policy.

6. Staff using BYOD must take all reasonable steps to:
   a. Prevent theft and loss of data
   b. Keep information confidential where appropriate
   c. Maintain the integrity of data and information
   d. Take responsibility for any software they download onto their device.

7. Staff using BYOD must:
   a. Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device
   b. Set up remote wipe facilities if available and implement a remote wipe if they lose the device
   c. Encrypt documents or devices as necessary
   d. Not hold any information that is sensitive, personal, confidential, or of commercial value on personally owned devices. Instead they should access information via the cloud services provided (webmail, Moodle, Quercus etc.) wherever possible
   e. Where it is essential that information belonging to the College 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. Emails should not be stored for longer than one month on a personal device
   f. Ensure that relevant information is copied back onto College systems and manage any potential data integrity issues with existing information
   g. Report the loss of any device containing College data (including email) to the Data Protection Officer (or their nominated deputy)
   h. Be aware of any Data Protection issues and ensure personal data is handled appropriately.
   i. Report any security breach to the Data Protection Officer (or their nominated deputy)
   j. Delete all data belonging to the College on leaving employment
   k. Ensure that College information is deleted from any personal device before it is disposed of, sold, or transferred to a third party.

## Monitoring and Access

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

a. Prevent access to a particular device from either the wired or wireless networks, or both
b. Prevent or restrict access to a particular system
c. Take all necessary and appropriate steps to retrieve information owned by the College.

### Data Protection and BYOD

9. Spurgeon's College collects, holds, processes and shares large amounts of personal data and has a legal obligation to ensure that it is kept secure and appropriately protected. In line with our Data Protection Policy, all staff have a duty to protect the personal data they possess from loss or unauthorised destruction, alteration, disclosure or access, whether due to human error or malicious intent. In some circumstances, the College has a legal responsibility to report personal data breaches to the Information Commissioners Office (ICO) within 72 hours of the time the breach occurred.

10. The College, 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 and using BYOD to process personal data.

11. A breach of the Data Protection Act, or its associated regulations, can lead to a significant fine for the College. Any member of staff found to have deliberately breached the Act or regulations may be subject to disciplinary measures.