Bring Your Own Device Policy (BYOD)

August 2019

Document Quality Control

Original

Version	Author	Date	Reviewed By	Date
March 2016	Taylor Partnership	March 2016	Taylor Partnership	March 2016

Document Reviews/Updates

Document Version Editing	Reason for Review/Update	Reviewer	Date	Checked / Approved By	Date
March 2016	Review and Update	Usman Ulhaq	March 2017	David Fear	March 2017
March 2017	Review and Update	David Fear	November 2018	Gareth Collier	January 2019
January 2019	Document Formatting	Cerys Williamson	August 2019	Gareth Collier	August 2019

Contents

Policy

1.0 Introduction

1.1 Cardiff Sixth Form College grants its employees and its students the right to using smartphones, tablets and laptops of their own choosing whilst in College. The College reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

1.2 This policy is intended to protect the security and integrity of Cardiff Sixth Form College's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

1.3 Members of the Cardiff Sixth Form College community must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the College network. They also agree to abide by all the terms and conditions laid down in the College's Acceptable use of ICT Policy.

2.0 Acceptable Use

2.1 A much more detailed list of conditions appears in the College's Acceptable use of ICT Policy. However, in broad terms, Cardiff Sixth Form College defines acceptable use as activities that directly or indirectly support the work of the College.

2.2 The College defines acceptable personal use of devices on College time as reasonable and limited personal communication or recreation, such as reading.

2.3 Members of the College community are blocked from accessing certain websites during work hours and while connected to the College network. The list of blocked websites is regularly reviewed and is compiled at the discretion of the senior management team.

2.4 Personal devices with camera and/or video capabilities should only be used by staff to photograph students when prior permission has been gained and all images are transferred to the College network and deleted from the devices within 72 hours. Students should only use such devices with the express permission of those they are photographing or in circumstances where a member of staff gives the necessary permission.

2.5 Devices may not be used at any time to:

- Store or transmit illicit materials
- Store or transmit sensitive information about any member of the Cardiff Sixth Form College community
- Harass others
- Engage in outside business activities

2.6 Most Apps will work on the College system. However, it is not the job of the College IT staff to unlock access to every conceivable App. The College knows that sufficient apps are operable to make use of a personal phone or device in College business.

2.7 Staff and students may use their mobile device(s) to access College e-mail and calendars and other elements of the Google Apps for education, family or software. However, where this is done, mobile devices **MUST** be passcode locked to prevent unauthorised access.

3.0 Devices and Support

3.1 Smartphones including iPhone, Android, Blackberry and Windows phones are all allowed. Tablets including iPad and Android are allowed. Connectivity issues are supported by IT; however, staff and students should contact the device manufacturer or their carrier for operating system or hardware-related issues.

4.0 Security

4.1 In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the College network.

4.2 The College's strong password policy is that passwords must be at least six characters and a combination of upper and lower-case letters and numbers. Passwords will be rotated every 90 days and the new password can't be one of 6 previous passwords.

4.3 The device must lock itself with a password or PIN if it's idle for five minutes.

4.4 Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.

4.5 Staff and student access to College data is limited based on user profiles defined by IT and automatically enforced.

4.6 If you use removable media to transfer data (USB drives or CDs), you must also consider the safe and secure deletion of the data on the media, once the transfer is complete as well as the password protection / encryption of any removable media.

4.7 You may want to consider disabling some of the interfaces which might be used to connect to other devices, such as Wi-Fi or Bluetooth, as these can be used to connect to a range of external peripherals such as a printer or other storage device. You should consider any conflict this may present with your current endpoint control policy.

4.8 Be aware some devices may offer an automated backup facility which stores a backup of data on the device to the user's cloud-based account or to the user's personal computer. You will need to ensure that, if this facility is enabled, it will not lead to an inappropriate disclosure of personal data.

5.0 Risks/Liabilities/Disclaimers

5.1 While the College will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.

5.2 The College reserves the right to disconnect devices or disable services without notification.

5.3 Lost or stolen devices **must be reported** to the Academic and Data Manager and GDPR Champion, Charlotte McQuaid, within 24 hours detailing the type of data that has been

lost. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

5.4 The employee is expected to use his or her devices in an ethical manner at all times and adhere to the Acceptable use of ICT Policy as outlined above.

5.5 Members of the College community are personally liable for all costs associated with their devices.

5.6 Members of the College community assume full liability for risks including, but not limited to, the partial or complete loss of College and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

5.7 The College reserves the right to take appropriate disciplinary action for noncompliance with this policy.

6.0 The Responsibilities of Staff Members

6.1 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 CSFC 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 College's Acceptable use of ICT Policy

6.2 While CSFC IT staff will always endeavour to assist colleagues wherever possible, the College cannot take responsibility for supporting devices it does not provide.

6.3 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 campus
- Take responsibility for any software they download onto their device

6.4 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 (see Protection of Information Held on Mobile Devices and Encryption Policy)
- Not hold any information that is sensitive, personal, confidential or of commercial value on personally owned devices.

- 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
- Ensure that relevant information is copied back onto College systems and manage any potential data integrity issues with existing information
- Report the loss of any device containing College data (including email) to the Academic and Data Manager / GDPR Champion.
- Be aware of any Data Protection issues and ensure personal data is handled appropriately.
- Report any security breach immediately to the Academic and Data Manager / GDPR Champion.
- Ensure that no College 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 Policy check and update

7.0 Monitoring and Access

7.1 The College 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 College

8.0 Data Protection

8.1 The College must process 'personal data' i.e. data about identifiable living individuals in accordance with the Data Protection Act 1998. 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.

8.2 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 using BYOD to process personal data.

8.3 A breach of the Data Protection Act can lead to the College being fined. Any member of staff found to have deliberately breached the Act may be subject to disciplinary measures, having access to the College's facilities being withdrawn, or even a criminal prosecution.