Clyst Vale
COMMUNITY COLLEGE
A Science, Maths and ICT Academy

Policy for Staff and Post 16 Student BYOD (Bring Your Own Device)

Date approved: 7th May 2015

Review Schedule: Annual

Reviewed:

Next review:

Context

Aims of this Policy

Definitions

CONTENTS

1. OVERVIEW

Staff and Parent/Student Agreement – Staff, parents and students must agree to the contents of this BYOD policy (using the form below) to show acceptance of the terms and conditions of the use of mobile electronic communication devices in the College before staff and students are permitted to use their own device.

Electronic Communication Device – such devices include laptops, netbooks and notebooks, iPads and tablets, Kindle and e-readers, iPod Touch, smartphone and mobile phones and any other devices that allow electronic communication. Devices that are primarily aimed at gaming or are primarily a music player are not allowed. Similarly, devices that just permit the making of phone calls and sending texts still come within the College Behaviour Policy. Clyst Vale Community College will make the final decision whether any such device is permitted.

Lost, stolen or damaged – Staff and students who bring such devices into College do so entirely at their own risk, just like any other personal item. Clyst Vale Community College will not accept any responsibility for devices that are misplaced, lost, stolen or damaged. Many devices have a location finder app and it is recommended that this feature is enabled to aid tracking where ever possible. It is also recommended that such devices are fully insured to cover loss and damage outside of the home.

Security and Care – Staff and Students are responsible for the proper care and use of their own device. Staff and students are responsible for the adequate security of their own device whilst in school, keeping it with them at all times when required or securing properly if they have a locker. It is recommended that staff and students do not share or lend their devices.

Educational use – Devices will only be used for educational purposes to support learning whilst in school. It will be at the teacher’s discretion as to when these devices may be used by a student within school lessons. Students will respect a teacher’s decision and turn off their device when requested to do so.

Audio, Photographs and Video – Staff and students will not use their device to record audio or take photographs or video of other students or members of staff without their permission. Staff and students should not transmit or upload such media without permission.

Internet Usage Policy – Devices will only access the internet through the Clyst Vale Community College network. Staff and students will adhere to the College’s ICT Acceptable Use Policy and ESafety Policy whilst on the College site. In addition, staff and students will not access any inappropriate material that may or may not already be downloaded onto their device. Members of staff have the right to access a student’s own device if there is reason to believe a student is in violation of this policy or the above mentioned policies.

Breaching the BYOD Policy – If a student breaches the BYOD Policy or if the College feels that there has been a breach then the student's device can be confiscated and held in the College office. The student's parent will be contacted and they will need to come into the College to collect the device. Subsequent breaches of this policy by the same student will result with that student no longer permitted to bring in their own device. Staff members will fall under the College Staff Policy for suspected policy breaches.

2. ABOUT THIS POLICY

2.1 We recognise that many of our staff and students have personal mobile devices (such as tablets, smartphones and handheld computers), which they could use for learning purposes, and that there can be significant benefits for both students and teachers, including increased learning flexibility, in permitting such use. However, the use of personal mobile devices for learning by staff and students gives rise to increased risk in terms of the security of College IT resources and communications systems and the protection of confidential information.

2.2 Anyone covered by this policy may use a personal mobile device for learning purposes, provided that they sign the declaration at the end of this policy and adhere to its terms.

2.3 This policy covers all Post 16 students on roll and all staff employed at Clyst Vale Community College.

3. PERSONNEL RESPONSIBLE FOR THIS POLICY

3.1 The Senior Leadership Team has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to Mr P Colin (Deputy Principal). Mr Colin and the College governors shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice.

3.2 Mr Colin has responsibility for ensuring that any person who may be involved with administration, monitoring, IT security or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.

3.3 All staff and students at Clyst Vale Community College are responsible for the success of this policy. Any misuse (or suspected misuse) of a device or breach of this policy should be reported to the ICT Network Manager in the first instance.

3.4 If you have any questions regarding this policy or have questions about using your device for learning purposes which are not addressed in this policy, please contact the ICT Network Manager.

4. SCOPE AND PURPOSE OF THE POLICY

4.1 This policy applies to staff and students who use a personal mobile device including any accompanying software or hardware (referred to as a device in this policy) for learning purposes. It applies to use of the device both during and outside school hours whilst on the College site.

4.2 This policy applies to all devices used to access our IT resources and communications systems (collectively referred to as systems in this policy), which may include (but are not limited to) smartphones, PDAs, tablets, and laptop or notebook computers.

4.3 When you access College systems using a device, the College is exposed to a number of risks, including the threat of malware (such as viruses, worms, spyware, trojans or other threats that could be introduced into our systems via a device). This could result in damage to College systems.

4.4 The purpose of this policy is to protect College systems while enabling you to access our systems using a device. This policy sets out the circumstances in which we may monitor your use of College systems, access your device and retrieve, remove or destroy data on it and the action which we will take in respect of breaches of this policy.

4.5 Breach of this policy may lead to the College revoking your access to College systems, whether through a device or otherwise. It may also result in sanctions up to and including exclusion and disciplinary actions. You are required to co-operate with any investigation into suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.

4.6 Some devices may not have the capability to connect to school systems. The College is not under any obligation to modify its systems or otherwise assist students in connecting to those systems.

5. CONNECTING DEVICES TO COLLEGE SYSTEMS

5.1 Connectivity of all devices is centrally managed by the Clyst Vale Community College IT Technicians, who must approve a device before it can be connected to College systems.

5.2 The College reserves the right to refuse or remove permission for your device to connect with College systems. Clyst Vale Community College IT Technicians will refuse or revoke such permission (and may take all steps reasonably necessary to do so) where in our reasonable opinion a device is being or could be used in a way that puts, or could put, the College, our students, our staff, our systems, or sensitive College data at risk or that may otherwise breach this policy.

5.3 In order to access College systems it may be necessary for Clyst Vale Community College IT Technicians to install software applications on your device. If you remove any such software, your access to our systems will be disabled.

5.4 At present, BYOD devices for staff and students will only connect to our wireless system in order to gain access to the internet. Access to the internal network is prohibited from BYOD devices for security reasons. Accessing the school system should be done using the College remote access server as if you were working from home. The internet access is filtered in the usual manner based on your College year group or staff status.

6. MONITORING

6.1 The College reserves the right to monitor, intercept, review and erase, without further notice, content on the device that is deemed to be in breach of this policy.

6.2 Monitoring, intercepting, reviewing or erasing of content will only be carried out in order to:

(a) prevent misuse of the device;

(b) ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy);

6.3 By signing the declaration at the end of this policy, you confirm your agreement (without further notice or permission) to such monitoring. You also agree that you use the device at your own risk and that the College will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.

7. SECURITY REQUIREMENTS

7.1 You must comply with our Student and Staff ICT Acceptable Use Policy which is available on the College website when using your device to connect to College systems.

7.2 The College reserves the right, without further notice or permission, to inspect your device and access data and applications on it, and remotely review, copy, disclose or wipe, enabling us to:

(a) inspect the device for use of unauthorised applications or software;
(b) investigate or resolve any security incident or unauthorised use of College systems;
(c) ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy).

You must co-operate with the College to enable such inspection, access and review, including providing any passwords or pin numbers necessary to access the device or relevant applications. A failure to co-operate with the College in this way may result in sanctions, up to and including expulsion or disciplinary procedures.

7.3 If the College discovers or reasonably suspects that there has been a breach of this policy, including any of the security requirements listed above, your access to College systems will be immediately removed.

7.4 By signing the declaration at the end of this policy, you consent to the College, without further notice or permission, inspecting a device and applications used on it, and remotely reviewing, copying, disclosing, wiping or otherwise using data on or from a device that is in breach of this policy.

8. LOST OR STOLEN DEVICES

8.1 In the event of a lost or stolen device, you should report the incident to the Post 16 administrator in the Post 16 office. Staff should follow procedures in the Staff Handbook.

9. APPROPRIATE USE

9.1 You should never access or use school systems through a device in a way that breaches this policy or the College's Student and Staff ICT Acceptable Use Policy.

9.2 If you breach these policies you may be subject to sanctions up to and including expulsion or disciplinary procedures.

10. TECHNICAL SUPPORT

10.1 Clyst Vale Community College do not provide any technical support for any personal devices. If you bring your device to school, you are entirely responsible for any repairs, maintenance, upgrades or replacement costs and services.

11. COSTS AND REIMBURSEMENTS

11.1 You must pay for your own device costs under this policy. By signing the declaration at the end of this policy you acknowledge that you alone are responsible for all costs associated with the device and that you understand that your usage of the device in school may increase your data usage charges.

12. DECLARATION AND AGREEMENT

I wish to use my personal mobile device for learning purposes at Clyst Vale Community College and explicitly confirm my understanding and agreement to the following:

- I have read, understood and agree to all of the terms contained in the Bring Your Own Device to School Policy.
- I understand that the terms of this policy will apply to me at all times, during or outside College hours, when I am on the College site.
- I acknowledge and agree that authorised personnel of Clyst Vale Community College shall have the rights set out in this policy, including but not limited to the right to access, monitor, review, record and wipe (as the case may be) data contained on my personal device (which I acknowledge may result in inadvertent access to or destruction of my personal data).
- I understand and agree that Clyst Vale Community College in its discretion may amend, or remove this policy at any time and that I will be bound by the terms of the policy as amended.

BYOD STAFF and PARENT/STUDENT AGREEMENT

Staff, parents and students - Please complete the acknowledgement form on your Parent Portal to agree to the contents of this policy. Students will be unable to use their own device in school unless both parties (parent and student) agree to the contents of this policy.

As a student I understand and agree to the conditions set out in the above BYOD Policy. I understand that if I breach this policy then my device may be removed and held in the school office to be collected by my Parent/Guardian. I also understand that I may lose the privilege of bringing my own device into school and possibly face sanctions.

As a Parent/Guardian I understand that my child will be responsible for adhering to this policy. I have read and discussed this policy with my child and they understand the trust and responsibility required in having their own device in school.

13. <u>This form is to be completed and signed in accordance with the BYOD Policy for Clyst Vale Community College</u>

IMPORTANT

- Only staff and Post 16 Students may use devices on the wireless network for the current academic school year.
- Staff and students will need to provide their device MAC address before access will be granted (see Page 3 for instructions).
- Staff and students should only **register ONE** device. If it is more useful to use an iPad wirelessly, then it would be prudent to connect the iPad rather than using your access key for your phone!
- **<u>DO NOT SHARE YOUR KEY</u>.** Keep it safe otherwise **<u>YOUR</u>** device will lose access to the network. The key will be revoked and another key will not be issued quickly!
- If you need wireless access for more than one device, you will need to state this on the form, and justify the reasons why.
- Devices are to be used for educational purposes only whilst adhering to the BYOD Policy
- If a device affects the operation of the College network in any way, it will be removed instantly.
- Setting up hotspots within the school is prohibited as it can affect the network
- File sharing apps and software is strictly prohibited
- Updates and apps should be installed outside of school to avoid any filter issues
- Devices should be fully charged prior to use in school as **<u>charging devices in the College is prohibited.</u>**
- In order to protect the network and mitigate BYOD devices to external threats, devices should always;
    1. utilise a personal firewall
    2. run anti-virus software and maintain any virus definition updates
    3. fully patched operating system with the latest service packs
    4. not run in ad-hoc mode, i.e. peer-to-peer mode

All staff and students requiring access to the wireless network must complete the form below. Students require a signature by a Parent/Guardian

STUDENT INFORMATION	
Name	
Staff/Year (12/13)	
Tutor Name	(If applicable)
DEVICE INFORMATION	
Primary Device type	Smartphone ☐ Tablet ☐ Laptop ☐
Device make	(ie iPad, Samsung Galaxy, Dell laptop)
MAC address	(See below how to get MAC address)
Second Device	(Please justify the need to have 2 devices attached to wireless)
Second Device type	Smartphone ☐ Tablet ☐ Laptop ☐
Device make	(ie iPad, Samsung Galaxy, Dell laptop)
MAC address	(See below how to get MAC address)
RESPONSIBILTY and CONSENT	
Use of the device:	
Parent/Guardian - I understand that the purpose of allowing my child to use their own device is to participate in teacher approved activities, only if the teacher permits. When not in lectures, the use of devices should be for school related work only. **All parties** - I understand that College wireless access is a privilege and this can be withdrawn if College policies are not adhered to. I agree with the Conditions of Use set out in the College BYOD policy	
Sign to agree	(Staff or parental signature)
Responsibility of device:	
Parent/Guardian - I understand that by using the device in school, Clyst Vale Community College is not responsible for any data loss, theft, damage or other associated costs for replacement or repair of equipment. My child is responsible for the device at all times **Staff/Student** - I understand that by using the device in school, Clyst Vale Community College is not responsible for any data loss, theft, damage or other associated costs for replacement or repair of equipment. **All** - I agree with the Conditions of Use set out in the College BYOD policy	
Sign to agree	(Staff or parental signature)
Date:	

HOW TO FIND YOUR DEVICE'S MAC ADDRESS

** Please consult your device manual if the instructions below do not match your device. We are unable to provide instructions for all versions of software

Apple iOS (iPad, iPhone, iPod)

- On the home screen, tap **Settings** > **General** > **About**
- Scroll down to **Wi-Fi Address**
- The **Wi-Fi address** is your MAC address (example: A3:B2:C1:D5:E2:F1)
- Copy this to the form above

Android Smartphone

- On the home screen tap the **Menu** key > **Settings** > **More** > **About Device** > **Status**
- Scroll down to **WiFi MAC address**
- Copy this to the form above

Android Tablets

- On the home screen tap the **Menu** key > **Settings**
- Scroll down and tap **About Tablet** > **Status**
- Scroll down to **WiFi MAC address**
- Copy this to the form above

Kindle

- On the home screen, press the **Menu** button
- Go to the **Settings** page
- Use the Kindle's 5-way controller to underline **Settings** and then press
- There will be numerous pages of personalised settings to customise the Kindle
- Search for **Device Info** to get your Kindle's **Wi-Fi MAC address**.
- Copy this to the form above

Windows 7 or Vista

- Type **CMD** in the search bar located above the start button and press **Enter**. This will open the command prompt.
- In the command prompt type **ipconfig**(space)**/all** (do not type space)and press **Enter**
- Under the section marked **Wireless LAN Adapter Wireless Network Connection**, look for **Physical Address**. This is your **MAC address**. (example: D3-2D-7D-03-23-3D)
- Copy this to the form above

Windows 8

- Locate the **search icon** on the right hand side of the screen and click on it.

- Type **CMD** in the search bar located above the start button and press **Enter**. This will open the command prompt
- In the command prompt type **ipconfig**(space)**/all** (do not type space)and press **Enter**
- Under the section marked **Wireless LAN Adapter Wireless Network Connection**, look for **Physical Address**. This is your **MAC address.** (example: D3-2D-7D-03-23-3D)
- Copy this to the form above

MAC OS X

- Click on the **Apple icon** on the top left corner of your screen
- Scroll down to **System Preferences** and click
- Select **Network** and choose **Airport**
- Click **Advanced** and navigate to the bottom of the page. Locate Airport ID. This is your **MAC address**
- Copy this to the form above

Review

This Policy will be reviewed regularly at by
Date adopted: