IT Mobile Device Usage Policy

1.0 Purpose

This document specifies the College policy for the use, management and security of all Mobile Devices that may access or hold College information.

2.0 Scope

2.1. This policy applies to all College issued Mobile Devices and personally owned Mobile Devices that are used to access West London College data and information, network or IT facilities including, but not limited to, College information systems, staff email, college managed network drive storage.

2.2. This policy applies to all Users which includes staff, contractors, consultants, agency workers and students operating on behalf of the College or undertaking College functions and thereby accessing the IT systems or who are provided with a College issued Mobile Device.

2.3. This policy only applies to students if they are carrying out a function on behalf of the College i.e. similar to a staff member's function.

2.4. Use of personally owned Mobile Devices to access and store College information, as well as a User's own personal content, is commonly known as 'bring your own device' or BYOD. BYOD is supported at the College via the WLC_OpenAccess wireless network service, for providing access to Internet services only; no access to internal resources is available via this network.

2.5. All personally owned Mobile Devices connecting to WLC_OpenAccess are treated as any other Internet connected unmanaged device, and users should take the same precautions in protecting data.

2.6. This policy recognises that personal Mobile Devices are and will be used to access College information but makes no comment on the requirement or recommendation to do so nor does it mandate or recommend the use of personal Mobile Devices.

2.7. The College is under no obligation to modify its systems to allow Users to connect their personally owned Mobile Devices to them where such modification may be required.

2.8. IT Services provides minimal Service Desk support (but not technician visits) for personally owned Mobile Devices, where this is necessary to enable Users to access College information or systems for business purposes.

3.0 Definitions

College issued Mobile Device means any Mobile Device that has been purchased, is owned or leased by the College regardless of the source of funding.

Personally owned Mobile Devices means any Mobile Device that is held personally by an individual in a private capacity.

For the purposes of clarification Mobile Devices include:

- Laptop computers
- Chromebooks
- Tablets
- Smart phones
- Portable storage includes removable hard disks, CDs, DVDs, memory cards and USB pen drives

Confidential information consists of information which, if disclosed or made publically available could damage commercial or financial interests, privacy, reputation or employability; could cause damage or distress to individuals; cause the College to not meet its legal obligations; or damage the College's reputation. The definition of Confidential includes any information which is either labelled as 'confidential' or, if not labelled 'confidential', would nevertheless be reasonably regarded as confidential.

4.0 Policy Statements

To maintain the integrity and protection of the College's IT Network all equipment connected to the IT Network must comply with a set of minimum standards. Poorly configured, managed or operated equipment may lead to serious degradation of network operation or a breach in network and systems integrity resulting in:

- Disruption to business as usual processes

- Disclosure of college information

- System or network compromise

4.1. The use of any Mobile Device to process and access College information creates risks including those relating to data protection, virus infection, and copyright infringement, unintentional or unlawful compromise of data and even loss or theft of device and/or data. The risks are increased, and are also more difficult to manage, when using personally owned Mobile Devices.

4.2. The College, and its staff, is required to process, and is committed to processing, all personal data in accordance with the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) (EU) 2016/679 regardless of the device used to access the information. Users are required to keep College information and personal data secure. This applies equally to College information held on College systems and devices or accessed/held on personally owned Mobile Devices.

4.3. The College reserves the right to refuse to allow access to particular devices or software where it considers that there is a security or other risk to its information or IT Network.

4.4. The College is the owner of all College information and the contents of College systems together with everything which is created on, transmitted to, received on or printed from, or stored or recorded on each Mobile Device, in each case during the course of the College's business or otherwise on the College's behalf – irrespective of who owns that Mobile Device.

4.5. The College reserves the right to request access to inspect, or delete College information held on a personally owned Mobile Device to the extent permitted by law and for legitimate business purposes. Every effort will be made to ensure that the College does not access the private information of the individual.

4.6. Monitoring of College IT activity logs whether using College issued Mobile Devices or personally owned Mobile Devices, will be carried out in accordance with the IT Acceptable Use Policy.

5.0 User Responsibility

Mobile Device Users are responsible for:

- The security of College information and of the device on which the information is held (see Data Access and Storage section for provisions regarding Confidential Information)
- Storing College information on the Mobile Device only for so long as necessary
- Deleting College information from the Mobile Device when no longer required or sooner if required by the College to delete it
- Ensuring, where possible, the device has up to date Operating System and anti-virus protection
- Complying with this policy and the related policies (specified in Related Documentation).

6.0 Data Access and Storage

6.1. Use of any personally owned Mobile Device for business purposes is at the User's risk and the College is not liable for any losses, damages or liability arising out of such use, including but not limited to loss, corruption or misuse of any content or loss of access to or misuse of such personally owned Mobile Device, its software or its functionality.

6.2. When storing and/or processing confidential information on a mobile device, use of a College issued Mobile Device (i.e. laptop or tablet) should always be seen as the preferred mechanism. Storage on personally owned Mobile Devices can put confidential information at risk of compromise and may be subject to varied technical standards, support, as well as access by third parties.

6.3. Confidential information should be stored within and accessed from College information systems and College managed storage to ensure security of and appropriate secure access to the information.

6.4. Confidential information should not be stored or transferred to a cloud computing service other than Google's G Suite or any such service unless it is under a College negotiated contract.

6.5. Only store the minimum amount of information necessary to carry out any required task on a mobile device. A temporary cache may be held on the device, therefore any confidential information should be deleted from the device as soon as the information is no longer required.

7.0 Device and Physical Security

7.1. Mobile Devices accessing College information must have a complex/strong password, passcode or PIN enabled to reduce opportunity for unauthorised access. Passwords, passcodes and PINs must be kept secure. The device should be set to automatically lock if inactive for 5 minutes or less, or locked manually.

7.2. Mobile Devices should, where possible, have operating system and anti-virus updates enabled. "Jailbroken" or "rooted" devices or those mobile devices which have otherwise circumvented the installed operating system security requirements, making them vulnerable to compromise, are not permitted to connect to the College's Network and systems.

7.3. College Issued Mobile Devices are configured to standard security and other settings before delivery to the User.

7.4. College issued Mobile Devices must not be left unattended whether on or off College premises and, where possible, must be physically locked away or secured.

7.5. College issued Mobile Devices must be uniquely identified, security marked (where possible), and linked to a User. Issue/loan records will be kept accurate and up to date.

7.6. The devices are College property and as such must be returned to IT Services upon change of User or termination of employment. They must not be sold, given away or otherwise be disposed of by the User.

7.7. IT Services will manage the re-image before re-issue to another User (or secure erasure when disposing of devices at end of life).

7.8. If devices are not returned the matter will be passed to Human Resources. The matter may also be passed to the Police for consideration of further action or for recovery via civil litigation.

7.9. For personally Owned Mobile Devices, employees must delete all College information from their device (on termination of their employment or, if the personally owned Mobile Device is repaired, exchanged, sold, given away or otherwise disposed of) and may be required to provide a written undertaking that this will be done. Without relieving employees of their obligation to delete all College information, the College's rights under paragraph 4.5 above apply, including after termination of employment.

8.0 Reporting Loss or Theft

8.1. In the event of loss or theft of any Mobile Device irrespective of whether it is a College issued Mobile Device or a personally owned Mobile Device (used to access College information, Network or IT systems), the User must act promptly to minimise the risk of compromise to College information by immediately:

- Changing their College network log-in password and notifying IT Service Desk of incident circumstances.

- Changing any other passwords that may have been used on the device (e.g. banking)

- Reporting theft of device to the Police

- Reporting loss or theft of mobile phone to the mobile network carrier directly.

8.2. Appropriate steps will be taken to ensure that College information on or accessible from the Mobile Device is secured, including remote wiping of the Mobile Device, where possible. The remote wipe will destroy all College data on the Mobile Device. Although it is not intended to wipe other data that is personal in nature (such as photographs or personal files or emails), it may not be possible to distinguish such information from College data in all circumstances. Users should, therefore, regularly backup all personal data stored on the Mobile Device.

9.0 Disciplinary Process

The College reserves the right to audit compliance with the policy from time to time. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with the College's Disciplinary Policy. Disciplinary action may ultimately lead to dismissal.

10.0 Deviations from Policy

Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation from or non-compliance with this policy shall be reported to the Head of IT Services.