VISION
West Nottinghamshire
College

MOBILE COMPUTING POLICY

INTRODUCTION

The purpose of this Policy is to describe the procedures and processes in place to ensure the secure use of the College's mobile computing devices and to protect devices and the data they may contain from unauthorised access or disclosure.

1. Scope

1.1 This policy applies to all employees, learners and any other person with access to mobile devices owned by West Nottinghamshire College and to all mobile devices used within and on behalf of the College.

1.2 Mobile devices in the context of this policy include laptop computers, mobile phones, tablets and other handheld devices capable of processing data.

1.3 The policy should be read in conjunction with the Transportation, Transfer and Sharing of Data Policy and the ICT & Information Security Policy.

2. Introduction

2.1 This policy provides guidance and instruction on the use of mobile computing devices and all users of such equipment must read, understand and comply with its requirements.

2.2 Any mobile device being used outside an office environment – for instance when the user is moving from one location to another – is obviously at greater risk than a desktop computer in an office in a secure building.

2.3 There are many additional risks to mobile devices that result from this way of working and users must be aware of these risks and adapt their behaviour accordingly.

2.4 Students and staff will wish to use their own devices to access their material on the College network and work related activities on the internet. This must be managed to ensure the security of personal data held by the College.

3. Responsibilities

3.1 Anyone allocated a mobile device must assume an appropriate level of responsibility for the device itself and the information stored on it, in accordance with the requirements of this policy.

3.2 Upon receiving a mobile device the user must complete a Mobile Computing Device User's Agreement (at Appendix 1 of this policy) confirming compliance with all applicable paragraphs of this Mobile Computing Policy.

3.3 Upon leaving the employ of West Nottinghamshire College or a change in roles or responsibilities which results in the user no longer requiring the mobile device, it must be returned to the IT Department. The IT Department remains responsible for the re-distribution of mobile devices. Upon returning the device the Mobile Computing Device User's Agreement (at Appendix 1 of this policy) must be signed off to release the individual from their responsibility for the device.

3.4 Any user intending to work off site with a mobile device must be aware of data protection and the risks of data loss. These are discussed in the Data Protection Policy, the ICT & Information Security Policy and the Transportation, Transfer and Sharing of Data Policy.

3.5 Users must take all reasonable steps to ensure no unauthorised persons have access to the mobile device or the data stored on it.

3.6 Users must take all reasonable steps to ensure that no unlicensed or malicious software is installed on the mobile device. Further information is available in the College's ICT & Information Security Policy.

3.7 Users must ensure any issued mobile device is brought into College for software updates, and PAT testing as required. All College owned mobile devices will be PAT tested every two years.

3.8 Loss Of Mobile Devices And Accessories
All users should take good care of their mobile devices and accessories to avoid any damage, loss or theft. The emphasis is on personal responsibility. In the event a user requires a replacement of lost, stolen or damaged equipment they may be liable for the cost of replacement if it is considered they have been negligent in their actions.

It is the responsibility of the user to contact the IT department at the College (Ext: 8001) in the event of a lost or stolen mobile phone or data device.

3.9 Return Of Mobile Devices, Data Devices, Sim Cards And Accessories On Leaving The College
It is important that all College equipment is returned to the IT Department at the end of your contract. Individuals will be responsible for any items not handed back directly to the IT department. When items are returned a return receipt will be issued. Failure to return items will result in charges being passed on to the employee.

4. Use of Mobile Devices

4.1 There must be a means of identifying all users of mobile devices that connect to the College internet or network.

4.2 Mobile devices issued to employees, members and other users remain the property of West Nottinghamshire College with the user assuming temporary "custodianship" of the device.

4.3 Mobile devices must only be used in line with the College Social Media Policy, and Email and Internet Policy.

4.4 If a problem is encountered with the mobile device The IT Department must be informed. If the problem compromises the security of the device it must not be used until either the problem is resolved, or authorisation is provided for resumed use.

4.5 Users must notify the police, appropriate line managers and IT if a mobile device is stolen.

5. Physical Security of College Issued Mobile Devices

5.1 All mobile devices must be maintained in an environment with an appropriate level of security to prevent unauthorised access to information stored on the device.

5.2 When not in use in College, all mobile computers must be retained in a secure environment. e.g. Do not leave items in a vehicle overnight.

5.3 All devices will be security tagged as soon as received into department or service, and then added to the appropriate inventory. Where tagging is inappropriate serial numbers will be recorded.

5.4 When mobile devices are taken from the main office or storage area all users must ensure that they take adequate precautions to protect the equipment against theft or accidental damage at all times.

5.5 Records must be maintained which detail mobile devices including type, serial number and software available, and include provision for signing out and return and copies of completed Mobile Computing Device User's Agreements (at Appendix 1 of this policy). The IT Team will maintain a central record of devices, but individuals are recommended to retain their own information as above.

5.6 Mobile devices must be carried as hand luggage and where possible disguised when travelling.

5.7 Mobile devices must have appropriate access protection, for example, passwords and encryption.

5.8 Mobile devices must not be left visible in an unattended vehicle at any time. Items should be transported in a glove box or in the boot of the car out of sight.

5.9 Manufacturers' instructions for protecting equipment must be observed at all times.

5.10 Care must be taken not to bump or drop the device and it should not be carried with objects that could damage it.

5.11 Items should not be placed on top of the device as it may not be able to support the weight.

5.12 A mobile device must not be exposed to extreme temperature changes. Cold temperatures can make components brittle and warm temperatures can cause them to melt or warp.

5.13 Care must be taken to keep liquids away from mobile devices.

6. Data Security When Using Mobile Devices

6.1 All College laptops must be encrypted. You should never share your password with any other user.

6.2 In the case of personal data the level of security forms part of the College's notification to the Information Commissioner under the Data Protection Act. This could be compromised if files are taken outside the workplace without appropriate measures being taken. Details of how to transfer data safely can be found in the Transportation, Transfer and Sharing of Data Policy.

6.3 Equipment carrying important, sensitive and/or critical business information must not be left unattended.

6.4 Users who travel with a College mobile device must make regular backups of any data it contains to the College network. Advice on making backups can be obtained from IT Support, Ext: 8001.

6.5 The mobile device must not be used to store passwords, safe/door combinations, or classified/sensitive information.

6.6 It is important when such devices are used in public places that care is taken to avoid the risk of being overlooked by unauthorised persons.

6.7 A mobile device must never be left unattended in public places.

6.8 Any mobile device capable of holding personal information must be protected with a PIN code to restrict entry.

7. Bring Your Own Device (BYOD)

7.1 The College recognises that staff, students and visitors may wish to use electronic devices they own while on College premises. The College is supportive of users utilising their own equipment but must ensure that people comply with Data Protection and Health & Safety legislation.

7.2 Mobile devices are used at the owner’s risk. The College will take no responsibility for accidents occurring as a result of the use of a personal device.

7.3 Users may charge mobile devices in College power outlets in order to maintain their use during their time onsite. However users are responsible for performing a visual inspection of their device including cables and leads to ensure that there are no visible signs of damage. User checks should be carried out before most electrical equipment is used, with the equipment disconnected.

Individuals should look for:-

- damage to the lead including fraying, cuts or heavy scuffing, e.g. from floor box covers;
- damage to the plug, e.g. to the cover or bent pins;
- tape applied to the lead to join leads together;
- coloured wires visible where the lead joins the plug (the cable is not being gripped where it enters the plug);
- damage to the outer cover of the equipment itself, including loose parts or screws;
- signs of overheating, such as burn marks or staining on the plug, lead or piece of equipment;
- equipment that has been used or stored in unsuitable conditions, such as wet or dusty environments or where water spills are possible.

Where there are any of these signs or anything else of concern then the device MUST NOT be connected to College power outlets.

7.4 Users must ensure their device and cables do not represent a trip hazard.

7.5 Users will be allowed to connect to the internet but will be subject to the normal College web filtering rules. Users are responsible for ensuring that their device is not used to access any illegal material or anything that would contravene the College Internet and Email Policy.

7.6 Users will be able to access the internet to assist them with their work or studies. Access to the College network including home directories will not be available on personal devices. Users will only be allowed to connect to the network using WiFi.

7.7 Users must enter their student/staff login credentials in order to access the internet on their device. This will allow tracking of all sites visited and enforcement of standard College web filtering.

7.8 Visitors are free to use their own devices subject to the requirements above. All visitors will be issued with a copy of the BYOD section of the Mobile Computing Policy if they request internet access, and will be issued with temporary login credentials.

7.9 Any staff wishing to use their own device to access College email MUST use a PIN code to protect that device if lost or stolen.

8.0 EDUROAM

8.1 West Nottinghamshire College has joined the Eduroam network and as such staff will be able to use the WiFi in any Eduroam hotspot around the world. These are frequently found in education establishments such as universities however the full list of available sites can be discovered using the 'eduroam companion' app available for both Apple and Android devices.

8.2 In order to access Eduroam, staff need to connect their devices to the WiFi point labelled "Eduroam" and enter their West Nottinghamshire College user id and password (just as if you were logging onto the network in a college building).

8.2 Under Eduroam rules: Users

- Are accountable to the organisations that issue them with their credentials (and to the law) for all use of such credentials and any activities undertaken with the authority of those credentials. In particular, users must not allow their own credentials, or network access authenticated by them, to be used by others. If the user believes that their credentials may have been compromised the user concerned must immediately report this to the IT team at West Nottinghamshire College (Ext. 8001).
- Must abide by restrictions applied by the home organisation and by Janet, including Acceptable Use Policies, Computing Regulations and Disciplinary Codes. Restrictions imposed by the visited organisations must also be respected. Where Regulations differ, the more restrictive applies.

9. Mobile Phones

9.1 Provision Of Mobile Phones And Accessories
The provision and approval of mobile telephones and accessories needs to be managed effectively.

The following guidelines should be adhered to at all times:

- The allocation of mobile phones and accessories should only be granted when accompanied by the approval of the appropriate line manager and appropriate director.
- As part of the College agreement all provision of mobile handsets and accessories must be made through the West Nottinghamshire College IT Department in accordance with the above authorisation.
- The College has identified three phone models which meet the needs of the business. A particular model of phone will be allocated according to the job role of the requester. Any requests for non-standard models and accessories will be declined.
- Before the issue of a mobile phone, the user will be required to sign an acceptance form agreeing to these policy guidelines.

9.2 Suggested Criteria To Consider For Issue Of A Mobile Phone

- Emergency first aid or child protection role (First Aid currently use radios)
- Key external liaison role with need to rove frequently off College sites
- Lone worker on frequent evening duties off site
- Key role with on-call / call-out responsibilities

Please consider, if a person occasionally needs a phone for a business journey, this should be requested from one of the pool phones available at a reception desk. Only in cases where a job role requires frequent travel will a permanent phone be issued.

9.3 Suggested Criteria To Consider For Issue Of A Data Bundle

Key external liaison role with need to rove frequently off College sites and to have constant access to emails and outlook calendar.

9.4 Use Of Handsets Whilst Driving

West Nottinghamshire College requires that mobile telephones are NOT used whilst driving. Use of a hands free kit while legal is discouraged. If a call is to be taken or made during a journey by car, then the member of staff should find a safe place to pull over, stop the engine and make or take the call as necessary.

9.5 International Roaming

Unless authorisation is granted by the line manager and functional director, all International mobile calls will be blocked. Lifting the bar with the mobile provider for a defined period can only be made by contacting the IT Department and with your line manager's approval, please note that a minimum of 48 hours' notice is required.

9.6 Premium Rate Calls

Calls made to premium rate numbers (prefix all 09 numbers) are barred. If, under monitoring, it is found that calls have been made to chat lines etc. this will be viewed as serious and may lead to disciplinary action. This also applies to premium rate SMS messages and will lead to removal of the SMS facility if abuse is detected.

9.7 Cost Control Measures

It is anticipated that the introduction of some of the above and the suggested guidelines below will help reduce mobile communication expenditure.

- Do not divert your office phone to your mobile.
- Do not request callers to contact you on your mobile when travelling abroad.
- Do not allow usage of your mobile by any other person, except in case of emergency.
- If you are in possession of a PDA when travelling abroad, keep downloads from the internet and email transactions to a minimum as these very quickly run up an expensive bill.
- Do not sign up to any paid for services with a monthly or annual bill

  There is the potential for each operating business group to introduce automatic cut-off levels for each mobile user.

However, all mobiles have the following barred:-

- *premium rate calls and SMS*
- *international roaming*

9.8 Billing

The College will receive a monthly consolidated invoice.

Itemised billing covering all individual usage will be available for viewing on line. If a line manager requires an individual log in please advise the IT Department.

9.9 Misuse Of Mobile Devices

The use of mobile phones detailed in this document may be monitored on a routine basis. Specific monitoring of individuals will be carried out to investigate any instances where the College has reasonable grounds to suspect misuse.

10. Training

10.1 Training will be available covering all aspects of the Mobile Computing Policy.

I have read and understood the College's attached Mobile Phone Policy and agree to be bound by its rules.

Signature:- ______________________________

Date:- ______________________________

IT Department Use

Name of member of staff in IT:-	
Signature:-	

Copy of <u>fully completed</u> form to kept in secure location by IT

MOBILE COMPUTING POLICY

College Owned Mobile Computing Device User’s Agreement

I agree to take responsibility for the College Owned Mobile Computing Device/s and associated peripherals detailed below. I have read the West Nottinghamshire College Mobile Computing Policy and agree to comply with its requirements.

The agreement will start when I sign this document below date of issue, and will terminate when I return the device and all associated peripherals and sign the Agreement below date of return.

User Information		
Name:	User ID:	Job Title:
Department:		Phone No:
E-mail:		

Equipment Information	
Make & Model:	Tag Number:
Peripherals: (List any peripherals issued with the device)	

Sign-off Information	
Date of issue:	Date of return:
User Signature:	User Signature:
Authorising Signature:	Authorising Signature:

MOBILE COMPUTING POLICY

Bring Your Own Device (BYOD) Policy – Copy for College Visitors

The College recognises that staff, students and visitors may wish to use electronic devices they own while on College premises. The College is supportive of users utilising their own equipment but must ensure that people comply with Data Protection and Health & Safety legislation.

Mobile devices are used at the owner's risk. The College will take no responsibility for accidents occurring as a result of the use of a personal device.

Users may charge mobile devices in College power outlets in order to maintain their use during their time onsite. However, users are responsible for performing a visual inspection of their device including cables and leads to ensure that there are no visible signs of damage. User checks should be carried out before most electrical equipment is used, with the equipment disconnected. Individuals should look for:-

- damage to the lead including fraying, cuts or heavy scuffing, e.g. from floor box covers;
- damage to the plug, e.g. to the cover or bent pins;
- tape applied to the lead to join leads together;
- coloured wires visible where the lead joins the plug (the cable is not being gripped where it enters the plug);
- damage to the outer cover of the equipment itself, including loose parts or screws;
- signs of overheating, such as burn marks or staining on the plug, lead or piece of equipment;
- equipment that has been used or stored in unsuitable conditions, such as wet or dusty environments or where water spills are possible.

Where there are any of these signs or anything else of concern then the device MUST NOT be connected to College power outlets.

Users must ensure their device and cables do not represent a trip hazard.

Users will be allowed to connect to the internet but will be subject to the normal College web filtering rules. Users are responsible for ensuring that their device is not used to access any illegal material or anything that would contravene the College Internet and Email Policy.

Users will be able to access the internet to assist them with their work or studies. Access to the College network including home directories will not be available on personal devices.

Users must enter their student/staff login credentials in order to access the internet on their device. This will allow tracking of all sites visited and enforcement of standard College web filtering.

Visitors are free to use their own devices subject to the requirements above. All visitors will be issued with a copy of the BYOD section of the Mobile Computing Policy if they request internet access, and will be issued with temporary login credentials.