Mobile Device Acceptable Use Policy

Owner: Director of Information and Learning Technologies
Issue Date: March 2016
Review Date: March 2018

Purpose
The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data from a mobile device connected to an unmanaged network outside of Colchester Institute's direct control. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet computers.
- Ultra-mobile PCs (UMPC).
- Mobile/cellular phones.
- Smartphones.
- PDAs
- Home or personal computers used to access corporate resources.
- Remote Desktop Service (VDI)
- Any mobile device capable of storing corporate data and connecting to an unmanaged network.

The policy applies to any hardware and related software that could be used to access corporate resources, even if said equipment is not corporately sanctioned, owned, or supplied.

The overriding goal of this policy is to protect the integrity of the private and confidential client and business data that resides within Colchester Institute's technology infrastructure. (Also refer to Colchester Institutes Data Protection Policy). This policy intends to prevent this data from being deliberately or inadvertently stored or accessed insecurely on a mobile device, home PC or carried over an insecure network where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the company's public image.
Therefore, all people using a mobile device connected to an unmanaged network outside of Colchester Institute's direct control to backup, store, and otherwise access corporate data of any type must adhere to company-defined processes for doing so.

Applicability
This policy applies to all Colchester Institute's employees, including full and part-time staff, hourly paid, students, contractors, freelancers, and other agents who utilize either company-owned or personally-owned mobile device to access, store, back up, relocate or access any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust Colchester Institute has built with its clients, supply chain partners and other constituents. Consequently, employment/enrolment at Colchester Institute does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

It addresses a range of threats to – or related to the use of – enterprise data:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive corporate data is deliberately stolen and sold by an employee.
Copyright	Software copied onto a mobile device could violate licensing.

Malware	Viruses, Trojans, Worms, Spyware and other threats could be introduced via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the enterprise to the risk of non-compliance with various identity theft and privacy laws.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT SERVICES. Non-sanctioned use of mobile devices to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the enterprise network.

Responsibilities
The Executive Director Human Resources at Colchester Institute has the overall responsibility for the confidentiality, integrity, and availability of corporate staff data.

The Executive Vice Principal Curriculum Planning and Quality at Colchester Institute has the overall responsibility for the confidentiality, integrity, and availability of corporate student data.

The Executive Vice Principal Finance and Corporate Development at Colchester Institute has the overall responsibility for the confidentiality, integrity, and availability of corporate data.

Other IT staff under the direction of the IT Services Manager are responsible for following the procedures and policies within IT Services.

All Colchester Institute employees/students are responsible to act in accordance with company policies and procedures.

Affected Technology
Connectivity of all mobile devices will be centrally managed by Colchester Institute's IT Services department and will utilize authentication and strong encryption measures. Although IT SERVICES is not able to directly manage external devices – such as home PCs – which may require connectivity to the corporate network, end users are expected to adhere to the same security protocols when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

Policy and Appropriate Use
It is the responsibility of any employee/student of Colchester Institute who uses a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct Colchester Institute business be utilised appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

Access Control
IT SERVICES reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure. IT SERVICES will engage in such action if it feels such equipment is being used in such a way that puts the company's systems, data, users, and clients at risk.

Prior to initial use on the corporate network or related infrastructure, **all college owned mobile devices must be registered with IT SERVICES.** IT reserves the right to withhold access to devices that have weak security or have been compromised.

All mobile devices attempting to connect to the corporate network through an unmanaged network (i.e. the Internet) will be monitored using technology centrally managed by Colchester Institute's **IT SERVICES** department. Devices that are not in compliance with the College IT security policy, or represent any threat to the corporate network or data will not be allowed to connect. Staff mobile, smart phones and tablet devices may only access the corporate network and data using the Remote Desktop Service (VDI) or email sync service.

Personal mobile devices may be connected to the network via the college Wi-Fi only though you are accepting responsibility for any interference or damage caused to or by your device.

Security
Employees using mobile devices and related software for network and data access **will**, without exception, **use secure data management procedures.** All mobile devices must be protected by a **strong password**, and all data stored on the device must be encrypted using **strong encryption**. See the Colchester Institute password policy for additional background. **Employees agree to never disclose their passwords to anyone**, particularly to family members if business work is conducted from home.

All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data. Any non-corporate computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by Colchester Institute's **IT SERVICES** department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.

Passwords and other confidential data as defined by Colchester Institute's **IT SERVICES** department are not to be stored unencrypted on mobile devices.

Any mobile device that is being used to store Colchester Institute data must adhere to the authentication requirements of Colchester Institute's **IT SERVICES** department. In addition, all hardware security configurations (personal or company-owned) must be pre- approved by Colchester Institute's **IT SERVICES** department before any enterprise data- carrying device can be connected to it.

IT SERVICES will manage IT security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Colchester Institute's overarching IT security policy.
Employees, contractors, students and temporary staff will **follow all enterprise- sanctioned**

data removal procedures to permanently erase company-specific data from such devices once their use is no longer required. In the event of a lost or stolen mobile device it is incumbent on the user to report this to IT SERVICES immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than IT SERVICES. If the device is recovered, it can be submitted to **IT SERVICES** for re-provisioning.

Employees, contractors, students and temporary staff will **follow** the Data Protection Act (DPA) 1988. The DPA applies to anyone who handles or has access to information concerning individuals and everyone in the workplace or working remotely has a legal duty to protect the privacy of information relating to individuals.

Help & Support
Colchester Institute's IT SERVICES department will support its sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT SERVICES department.

Employees, students, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of Colchester Institute's IT SERVICES department. This includes, but is not limited to, any reconfiguration of the mobile device.

IT SERVICES reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

Organisational Protocol
IT SERVICES can and will establish audit trails and these will be accessed, published and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to Colchester Institute's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains Colchester Institute's highest priority.

The **end user agrees to immediately report** to his/her manager and Colchester Institute's IT SERVICES department **any incident or suspected incidents of unauthorised data access**, data loss, and/or disclosure of company resources, databases, networks, etc.

Colchester Institute will not reimburse employees / students if they choose to purchase their own mobile devices. Users will not be allowed to expense mobile network usage costs. Every mobile device user will be entitled to a training session around this policy. While a mobile device user will not be granted access to corporate resources using a mobile device without accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

Any questions relating to this policy should be directed to Mark Harrod, IT Services Manager, on 01206 712217 or Mark.Harrod@colchester.ac.uk.

Policy Non-Compliance
Failure to comply with the Mobile Device Acceptable Use Policy (this policy) may, at the full discretion of the organisation, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

The (i) Executive Director Human Resources, (ii) The Executive Vice Principal Curriculum Planning and Quality and (iii) immediate Line Manager/Head of Centre will be advised of breaches of this policy and will be responsible for appropriate remedial action which may include disciplinary action, including suspension or termination of employment.

	Date	Comments
Approval		
Review	10/03/2015	Default: 3 years from effective date

Employee Declaration

I, ……(Employee) have read and understand the above Mobile Device Acceptable Use Policy, and consent to adhere to the rules outlined therein.

_____ _____

Employee Signature Date

_____ _____

Managers Signature Date