East Dunbartonshire Council
www.eastdunbarton.gov.uk

Mobile Devices Policy

East Dunbartonshire Council
www.eastdunbarton.gov.uk

Version Control

Author:	Iain Stewart
Owner: (This field must specify the senior responsible officer and their department)	ICT Manager Vince McNulty
Source Location:	H:\PUBLIC\BC&IS\01. Information Security\01.04 Policies, Procedures, Manuals and Forms\FOR REVIEW\Ready for Group\Mobile Working Policy - v0.7.doc
Other Documents Referenced:	
Related Documents:	
Contact:	Iain Stewart iain.stewart@eastdunbarton.gsx.gov.uk 0141 578 8035 07766424497

Change History

This document is subject to change control and any amendments will be recorded below.

Version	Date	Changes	Author	Authorised
0.1	10/05/2006	Initial draft	ST (Sapphire)	
0.2	31/08/2006	Initial draft – completed	ST (Sapphire)	
0.3	31/02/2007	EDC amendments and additions by H Mofidian	HM	
0.4	24/04/2007	Revisions by PE	PE	
0.5	03/07/2007	Revisions by PE	PE	
0.6	19/07/2007	Asset form added	PE	
0.7	22/01/2008	Changes made in line with IS Group's comments	PE	
1.0	22/08/2008	Final version for P&R	PE	
2.0	25/09/08	Approved by P&R	PE	
3.0	27/02/09	Addition at 2.1 to read: *Teaching staff may attach personal USB devices to Council ICT facilities in pursuance of their duties to the council.* Addition to 5.3 to read: *Users should only ever access PROTECT and RESTRICTED information from a non-EDC device when it is essential to do so.*	PE	CMT

		CONFIDENTIAL material must only be accessed on a privately owned device in exceptional circumstances for example, to prevent an immediate incident. Addition to 5.5 to read: *Under no circumstances should encryption keys or passwords be written down or stored with any device.*		
3.1	05/11/2012	Author changed from Peter English to Iain Stewart and owner changed from Information Security Group to ICT Manager, Vince McNulty	Iain Stewart (IS)	
3.2	06/11/2012	Updated to reflect recent changes to Blackberry Policy and incident management procedures, removal of appendix A, form no longer required.	IS	
3.3	7/11/2012	Remove of 5.6 encryption software roll out now complete	IS	

Version Awareness

This document may not be the latest available version. The latest version, which supersedes all previous versions, is available at: <LINK>

1 Introduction

Mobile devices such as laptop computers or BlackBerries offer a portable and convenient mobile working solution and provide obvious business benefits to users, however, the mobile nature of these devices increases the risks of loss or theft of the device and any data it contains.

Risks are higher because:

- Laptops are an attractive target for thieves and are easily lost;
- Laptop or BlackBerry screens can be viewed by unauthorised parties if used in public;
- Domestic premises are more likely to be targeted by thieves and physical security in the home tends to be weaker than corporate premises;
- Data can remain on mobile or remote devices even if a user has attempted to delete it;
- The Council cannot guarantee the security of third parties' devices and information which has been viewed on remote devices is therefore more vulnerable;

In order to reduce these risks users should follow the advice below.

Compliance with this policy will minimise the risks to information that is being stored, processed or transmitted outwith Council premises and assist the Council in discharging its duty of care to citizens and employees.

1.1 Scope:

This policy applies to any employee or Elected Member (henceforth known as 'users') of East Dunbartonshire Council with access to a Council owned mobile device.

This policy sets out controls on the use of mobile devices which are defined as any device capable of processing digital information such as laptops, tablet PCs, PDAs and BlackBerries and also privately owned devices that are used to create, store, process or transmit Council information.

This policy is designed to mitigate the risks to Council information on mobile and remote devices by educating users on how best to treat their mobile devices and the information stored on them.

Users are responsible for reading understanding and adhering to the requirements of this policy. Heads of Service and Service Managers have the additional responsibility of implementing this Policy within their respective teams and for overseeing compliance by their staff.

1.2 Compliance with this policy

Failure to comply with this policy may result in disciplinary action being taken under the Council's disciplinary procedures. If there is anything in this policy that you do not understand, please discuss it with your line manager or contact the Information Security Manager for advice.

Please note that the controls outlined in this policy and in related policies, may be reviewed or changed at any time. Users will be alerted to important changes, and updates will be published on the Council's intranet.

Employees and Elected Members must sign the form contained in the Acceptable Use Policy to indicate that they understand, and will abide by, the contents of this policy.

2 Responsibilities of All Mobile and Remote Workers

2.1 General Responsibilities

Users are responsible for safeguarding Council-owned mobile devices that have been issued to them. Best endeavours must be made to reduce the possibility of loss or theft of Council-owned mobile devices.

Users are responsible for ensuring that information which would be classified as PROTECT, RESTRICTED, or CONFIDENTIAL is not taken out of Council premises unless encrypted on an approved Council USB stick or on an approved, encrypted Council laptop PC.

Laptops **must** be shutdown and / or switched off when not in use. This ensures that any encryption solution installed is protecting the laptop and also helps to prevent damage to the hard-drive. Even encrypted laptops are vulnerable when left switched on.

Users assigned a Council-owned mobile device are responsible for preventing unauthorised persons from using them (such as friends and family members), users must not loan them to others without prior authorisation via the Mobile Device Authorisation Form.

It is not permitted to connect personal mobile devices or personal equipment such as USB sticks to Council devices. Only council approved encrypted USB drives and Council supplied Blackberry's may be connected.

Teaching staff may attach personal USB devices to Council ICT facilities within the school estate in pursuance of their duties to the council and only for the use of material that is NOT PROTECTIVELY MARKED.

Information which would be classified as PROTECT, RESTRICTED, or CONFIDENTIAL must not be stored, processed or transmitted on or via personal computing devices.

Users are responsible for ensuring that unauthorised third parties do not gain access to Council information, such as committee reports, stored transmitted or processed on privately-owned computers.

Mobile workers must take heed of the environment in which they are working and apply appropriate common-sense measures to protect Council-owned portable computers and Council data on both Council-owned and privately-owned devices.

2.2 Data Protection requirements

Citizens and employees entrust their data to the Council. It is the individual responsibility of users to protect the personal data of others and only use it for the purposes for which it was given to the Council.

The unauthorised disclosure, modification or loss of citizens' or employees' data could result in the prosecution of individuals for breach of the Data Protection Act 1998. It is therefore essential that users familiarise themselves with their responsibilities under the Data Protection Act and they should refer to the Council's Data Protection and Information Classification and Protection Policies for further advice.

Databases containing the personal information of employees or members of the public must not be stored on unencrypted mobile devices or USB sticks. Such databases must only be taken off the Council's network when there is a clear business or statutory requirement and they must only be stored on approved encrypted devices.

The personal information of citizens or employees of East Dunbartonshire Council must not be stored on personal devices.

2.3 Data Backup

All mobile and remote workers are individually responsible for regularly 'backing-up' Council data which they have stored, or caused to be stored, on any device. Data that users wish to back up must be stored on the Council's network.

2.4 Incident reporting

The loss or theft of any Council-owned information asset must be reported to relevant line manager and the ICT Service Desk as soon as possible. No longer than 1 full working day.

If the loss or theft took place from an Employee home, car or location external to the Authority then the incident must be reported to the police as soon as

possible and no longer than 1 full day and the relevant incident or crime reference numbers passed to the ICT Service Desk.

If a Council mobile device is lost or stolen, the sensitivity of the lost information should be assessed, in accordance with the Incident Investigation Procedure, to determine the potential impact on members of the public, employees and the Council's reputation. Any mitigating actions can then be assessed and implemented.

Loss or damage to, Council-owned portable computers may be investigated in accordance with the Incident Investigation Policy. Where negligence on behalf of the custodian has resulted in the loss or damage disciplinary action may be taken in accordance with Council procedures.

2.5 Scenario-based controls

The main scenarios in which users will find themselves are:

- working within Council premises;
- working outwith Council premises;
    - in public;
    - from home; and
    - on holiday / abroad

Control requirements associated with each of these are outlined below.

2.5.1 Working within Council premises

Council-owned portable devices should not to be left unattended on Council's premises unless they are behind a secure perimeter, i.e. in a locked room or locked drawer.

If working from a Smart Working Environment when leaving your Laptop for any period of time you must lock your device to prevent any unauthorised access. This can quickly be done by pressing the "windows" key and the "L" key

2.5.2 Working outwith Council premises

When working outside Council premises, mobile workers must take extra care and take appropriate measures to protect portable devices in their care.

2.5.3 Using mobile devices in public places

When using a mobile device in a public place users must take extra care to prevent the disclosure of Council information. Screens should be positioned so that information is not visible.

CONFIDENTIAL, RESTRICTED or PROTECT information must not be accessed in places where a screen could be overlooked by an unauthorised party.

If portable devices have to be left in vehicles, they must be switched off and placed out of sight in the boot or out of sight under a seat and the vehicle locked.

To reduce the possibility of the theft of Council-owned mobile devices users carrying laptops may prefer to use 'disguised' laptop bags so that it is not obvious what they are carrying.

2.5.4 Using mobile devices abroad

Mobile Devices can be used as per the rest of the policy within European Economic Area (EEA[1]) countries.

2.5.5 Mobile and Remote Working outwith the European Economic Area

The Data Protection Act 1998 prohibits the international transfer of personal data to any country outside the EEA, without the explicit consent of the individual. Any negligent action, which led to the transfer of personal data outwith the EEA, could render a user liable to prosecution under the Data Protection Act 1998.

3 Responsibilities of Heads of Service

Heads of Service are responsible for ensuring that all mobile and remote workers in their Service understand and sign up to this policy. In addition Heads of Service must ensure that mobile devices, owned by their Service are assigned according to this policy and that devices are updated frequently and regularly by ICT.

3.1 Controls on the allocation of mobile devices

The allocation of mobile and SMART devices to staff are recorded and marked using the councils asset bar-coding system and also added to the central asset management register.

These details are also recorded manual by the Service Desk on a mobile asset register.

3.2 Returning mobile devices to ICT for updates

Mobile Devices must be returned promptly to ICT as part of any update programme.

[1]Currently: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Liechtenstein, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

4 Responsibilities of ICT and Information Security Manager

4.1 Approved technologies

All devices used to create, store, process or transmit 'sensitive information', as specified by the Council's Information Classification and Protection Policy, must be approved by the Information Security Manager and the Corporate ICT Services Manager.

4.2 Incident reporting and investigation

The Information Security Manager is responsible for ensuring that a log of all incidents involving mobile devices is maintained and reported to the Information Security Forum.

The Information Security Manager may request that a line manager conducts an investigation into the loss of, theft of, or other incident involving a mobile device.

4.3 Register of mobile devices

Windows based mobile computing resources and devices where a client is available have the council's asset management client automatically installed which registers and periodically updates both from internal council network IP addresses and external IP address to its Management and Reporting Server.

Non Windows based devices or devices where a client is not currently available are recorded using the asset bar-coding system and the details manually transferred and recorded within the central asset management database

The following details are recorded.

Field	Example
Device Name	2C204661H
Device Type	Laptop Computer.
Model Number	PORTEGE R830 PT320E-0JJ01REN
Location	Location of asset based on IP address
Serial Numbers	A list of all serial numbers
Mac Address	Mac address of installed network adapters
IP Address	IP Address of machines during audit
Last Contact	Time and date of last contact
Last Audit	Time and date of last audit
Hardware Details	Various hardware details, from memory, processors and cores, hard drives, network adapters, video and audio cards, optical drives etc
Device Owner	User name
Installed Software	List of installed software and applications
File Types	Comprehensive list of files types on the machines and they disk space they use
Audit History	Visible Audit History
Change Alerts	Notification of Hardware or location changes
Print Options	Print out the asset information
Report Options	Export as Excel or PDF

5 Access Scenarios

5.1 The Remote Access to the Council's Network via 'The Portal'

All devices connecting remotely to the corporate network must utilize a corporate-approved Virtual Private Network (VPN), which is configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, implementations must maintain point to point encryption using Council approved cryptographic standards and algorithms to at least 128bits. The currently recommended minimum standard is 128bit AES.

All implementations must support a hardware address that can be registered and tracked – e.g. a MAC address. Implementations should support the deployment of 2 factor authentication such as RSA SecurID which checks against an external database such as RSA ACE Server or similar.

Users can read and reply to emails using The Portal but sensitive material or documents must not be saved or downloaded to personal computing equipment. Passwords for Portal access must not be written down or stored on a remote or mobile device.

5.2 The Remote Access to the Council's Network via a BlackBerry

Users are responsible for their own BlackBerry handheld, and all actions carried out upon it. They should not allow any other individual to use their handheld for any reason.

When BlackBerries are first issued a default password is set. Users should change this as soon as they have acquainted themselves with their device's functions. The password change feature can be found under: Settings: Security Options: General Settings: Password: Change Password.

The current East Dunbartonshire Policy requires the following

- Be at least 7 characters in length;
- Contain a mixture of letters, numbers and special characters[1];
- Be as random as possible, and in particular must not contain recognisable words or any other strings associated with the user; and
- Should not contain more than two consecutive identical characters.

In addition users should adhere to the following guidance relating to the choice and use of passwords:

- Do not use the same password for a BlackBerry handheld as for any other system
- Never, for any reason, disclose BlackBerry passwords to anyone, be that in person, by phone, or by email

[1] ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | }

- If the BlackBerry password is written down, it must be placed in an envelope marked RESTRICTED and treated accordingly (i.e. kept in a secure cabinet).
- Under no circumstances should a written copy of the password be carried along with the handheld.

Users should note that the email and calendar functionality available on the BlackBerry is essentially an extension of the Council's email network and as such all usage is subject to the Council's Acceptable Use of ICT Facilities Policy.

Users may open attachments on received emails, but, as with standard email services, should avoid opening any attachments which are unexpected or from an unfamiliar source.

Users must not use personal BlackBerry cradles and should ensure that their device is only ever connected to Council owned devices and computers on the Council's network. BlackBerries should never be connected to a user's own personal computer or another network.

If a user believes that their handheld is in immediate danger of theft or compromise, and wishes to erase all sensitive data from the device, this can be done via the "Wipe Handheld" option by following this path *Settings: Security Options: General Settings: Password: Wipe Handheld*.

5.3 Council Information on Privately-owned Computers

Privately-owned computers **must not** be used to create, store, or transmit information which would be classified as CONFIDENTIAL, RESTRICTED or PROTECT under the Council's Information and Classification Policy.

Users should only ever access PROTECT and RESTRICTED information from a non-EDC device when it is essential to do so. CONFIDENTIAL material must only be accessed on a privately owned device in exceptional circumstances for example, to prevent an immediate incident.

5.4 Protection of Privately Owned Computers Containing Council Information

Users, who access, produce or store non-sensitive Council information on privately owned computing devices, whether portable or not, are responsible for that device's security. To properly protect Council information, such devices are to be protected by a recognised, up-to-date firewall and anti-virus solution, and be kept up to date with security patches. Council information must be securely deleted from the device using a recognised disk sanitization tool. The Information Security Manager is available to give advice in this area.

Under no circumstances should encryption keys or passwords be written down or stored with any device.

East Dunbartonshire Council

www.eastdunbarton.gov.uk