URBS · IN · RURE

Solihull
METROPOLITAN
BOROUGH COUNCIL

Policy on the use of Portable ICT Equipment

Version 2.1 – December 2009

VERSION

Title: Policy on the use of Portable ICT Equipment

Current version: 2.1

Document type: Published

Prepared by: Andrew Shipway / Hilary Staton

Approved by: N/A

Review date: January 2011

Circulation: Employees issued with portable ICT equipment

Document revision dates

Revision	Date	Revision description
1.0	March 2003	Original Policy
1.1	June 2007	Complete rework to bring it in line with BS7799 standards
1.2	Sept 2007	Amended to take account comments of the End User Support Manager
1.3	November 2007	Amended to take account of comments by Financial Manager - Treasury Mgt & Insurance re: Insurance arrangements
2.0	December 2008	Amended as part of the Council's preparations for compliance with the Governments Code of Connection (CoCo)
2.1	December 2009	Amended tips on what password formats to use to use

PO Box 18
Council House
Solihull
West Midlands
B91 9QS

CONTENTS

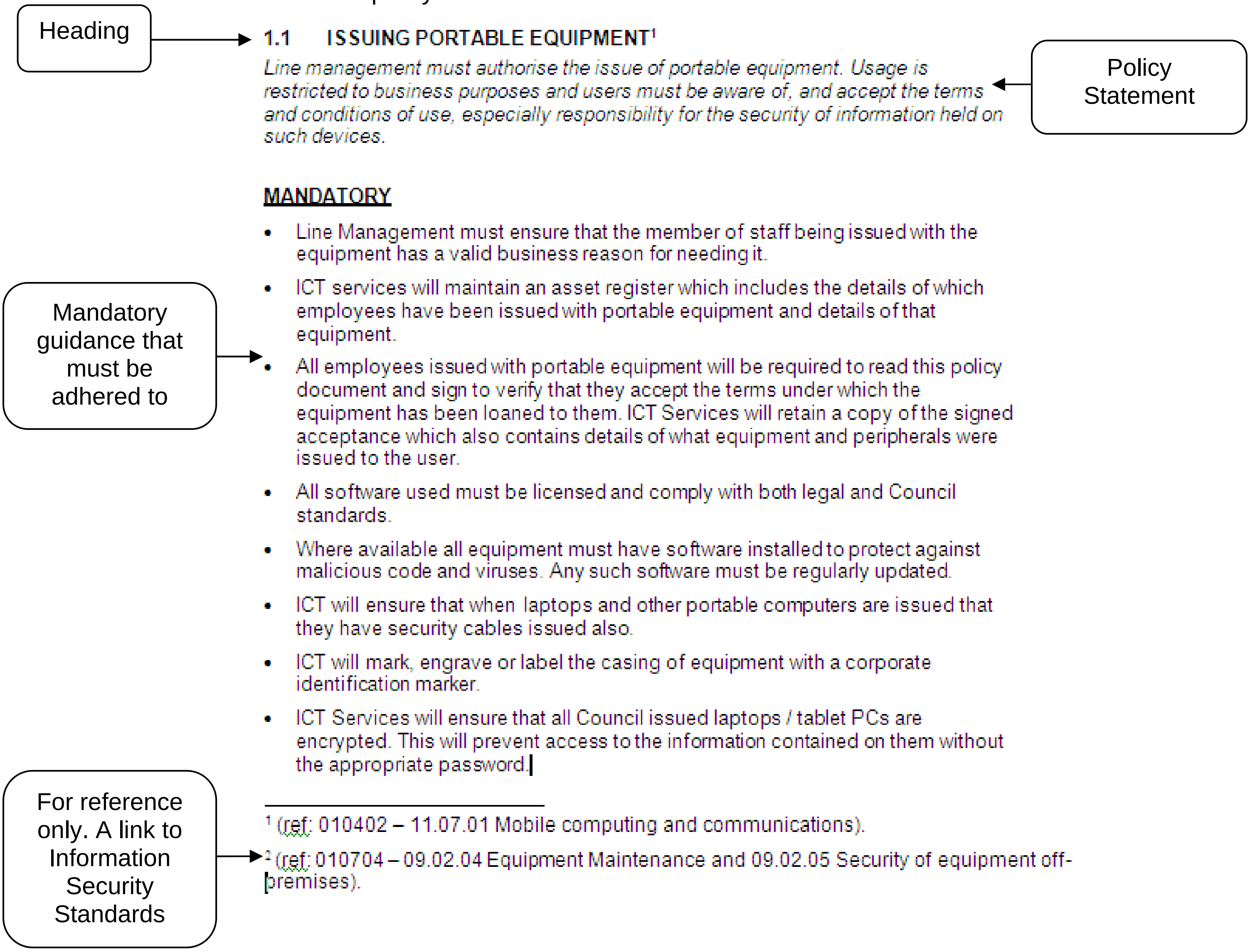
USE OF PORTABLE EQUIPMENT

APPENDIX A

APPENDIX B

HOW TO USE THIS DOCUMENT

The format of each policy statement is illustrated below.



Heading

1.1 ISSUING PORTABLE EQUIPMENT[1]

Line management must authorise the issue of portable equipment. Usage is restricted to business purposes and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devices.

Policy Statement

MANDATORY

- Line Management must ensure that the member of staff being issued with the equipment has a valid business reason for needing it.
- ICT services will maintain an asset register which includes the details of which employees have been issued with portable equipment and details of that equipment.
- All employees issued with portable equipment will be required to read this policy document and sign to verify that they accept the terms under which the equipment has been loaned to them. ICT Services will retain a copy of the signed acceptance which also contains details of what equipment and peripherals were issued to the user.
- All software used must be licensed and comply with both legal and Council standards.
- Where available all equipment must have software installed to protect against malicious code and viruses. Any such software must be regularly updated.
- ICT will ensure that when laptops and other portable computers are issued that they have security cables issued also.
- ICT will mark, engrave or label the casing of equipment with a corporate identification marker.
- ICT Services will ensure that all Council issued laptops / tablet PCs are encrypted. This will prevent access to the information contained on them without the appropriate password.

Mandatory guidance that must be adhered to

[1] (ref: 010402 – 11.07.01 Mobile computing and communications).

[2] (ref: 010704 – 09.02.04 Equipment Maintenance and 09.02.05 Security of equipment off-premises).

For reference only. A link to Information Security Standards

INTRODUCTION AND SCOPE

Introduction

- The purpose of this policy is to ensure employees understand the Council's guidelines and expectations for the use of portable ICT equipment. Such equipment includes laptops, tablet PCs, Personal Digital Assistants (PDAs) and Blackberrys.

- Failure to comply with this policy may result in disciplinary action being taken against you under our disciplinary procedures, which may include summary dismissal, or the withdrawal of permission to use the Council's equipment. If there is anything in this policy that you do not understand, please discuss with your Line Manager or contact the Corporate Information Governance Manager.

- The procedures and policies outlined in this document, and in any related policy, may be reviewed or changed at any time. You will be alerted to important changes, and updates will be published on the Corporate Performance and Policy area of the Intranet.

Scope

- This policy applies to anyone who uses portable ICT equipment owned by the Council. This includes partner organisations, staff who work full or part-time, or under temporary contracts, contractors and elected officials.

1. USE OF PORTABLE ICT EQUIPMENT

1.1 BACKING UP DATA[1]

Information stored on laptops, tablets and other types of portable computer must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.

MANDATORY

- Information that is of significant value, or perhaps private and confidential may be lost due to system failure or loss/theft of equipment. Therefore, all computer systems and their associated data files must have agreed backup and restore procedures.
- Where possible use inbuilt features of the system being used, e.g. Microsoft Windows ® 'Briefcase' or 'Make Available Offline' to allow data files to be modified and synchronised automatically when re-connected to the Council's network.
- The user of the equipment will be responsible for ensuring such backups take place on a regular basis.
- Equipment should hold the bare minimum of information needed to perform the task in hand. Therefore, when backing up information, users should ensure that any old / no longer needed information is removed as part of the backup process.

1.2 ISSUING PORTABLE EQUIPMENT[2]

Line management must authorise the issue of portable equipment. Usage is restricted to business purposes and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devices.

MANDATORY

- Line Management must ensure that the member of staff being issued with the equipment has a valid business reason for needing it.
- ICT services will maintain an asset register which includes the details of which employees have been issued with portable equipment and details of that equipment.
- All employees issued with portable equipment will be required to read this policy document and sign to verify that they accept the terms under which the equipment has been loaned to them. ICT Services will retain a copy of the signed acceptance which also contains details of what equipment and peripherals were issued to the user.
- All software used must be licensed and comply with both legal and Council standards.
- Where available all equipment must have software installed to protect against malicious code and viruses. Any such software must be regularly updated by

[1] (ref: 030602 – 11.07.01 Mobile computing and communications).

[2] (ref: 010402 – 11.07.01 Mobile computing and communications).

connecting the laptop/portable equipment to the Council's computer network at least once a month.

- ICT will ensure that when laptops and other portable computers are issued that they have security cables issued also.
- ICT will mark, engrave or label the casing of equipment with a corporate identification marker.
- ICT Services will ensure that all Council issued laptops / tablet PCs are encrypted. This will prevent access to the information contained on them without the appropriate password.

1.3 INSURING LAPTOPS / PORTABLES FOR USE DOMESTICALLY OR ABROAD[3]

All portable equipment is to be insured to cover use in the UK or abroad.

<u>MANDATORY</u>

- The Financial Manager - Treasury Mgt & Insurance is responsible for ensuring adequate insurance is in place.
- When equipment is used at home it is expected that reasonable care is taken of it. Failure to take reasonable steps to look after the equipment will mean that any claim for loss or damage to the equipment will not be covered by the Council's insurance arrangements.
- The Council's insurance arrangements have an excess of £500 for all losses. These excesses are charged to directorate budgets.
- If equipment is to be taken abroad the Financial Manager – Treasury Management & Insurance should be contacted to ensure there is adequate insurance cover.

<u>Exclusions</u>

The usual exclusions apply to the Council's insurance arrangements, including:

- losses through general wear and tear etc.
- losses from items left unattended and on show in motor vehicles
- Losses from damage caused by a lack of 'reasonable care' of the item, e.g. insecure storage of the item at home, left on view etc.

[3] (ref: 010704 – 09.02.04 Equipment Maintenance and 09.02.05 Security of equipment off-premises).

1.4 DAY TO DAY USE[4]

Portable ICT equipment is to be issued to, and used only by, authorised employees and only for the purpose for which it is issued. The information stored should be suitably protected at all times.

MANDATORY

- Because of their size and value portable ICT equipment such as laptops make attractive targets for thieves. There are two main areas of concern for those using such equipment:-
  - Avoiding the loss or theft, and
  - Protecting sensitive/confidential data in case of theft.

- Portable ICT equipment should never be connected to any ‘home network’ or directly to the Internet, unless this has been set-up and agreed by ICT services.

- Always use a strong password that is impossible to guess[5].

What Not to Use

- Don't use your login name in any form e.g. 'as is', reversed, capitalized, doubled, etc.
- Don't use your first or last name in any form.
- Don't use your spouse or partner's name; or that of one of your children.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, your home or street name etc.
- Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a hacker.
- Don't use a word contained in the dictionary (English or foreign language), spelling lists, or other lists of words.
- Don't ever use a password shorter than six characters.

What to Use

- Use a password at least eight characters in length with a mixture of mixed case alphabetic characters and non alphabetic characters, e.g., digits or punctuations.
- Use a password with non alphabetic characters, e.g., digits or punctuation.
- Use a password that you are able to commit to memory; so you don't have to write it down.

[4] (ref: 010408 – 09.01.02 – 11.07.01 Mobile computing and communications).

[5] (ref: 030810 – 11.01.01 Access control policy).

1. USE OF PORTABLE ICT EQUIPMENT

Tip: The easiest way to create a password is to think of a phrase that is complex and meaningful to you, and then tailor it accordingly to ensure there are enough characters in it of the right mix. For example, select the first letter of each word. For example, "My son Aiden is three years older than my daughter Anna", would create the password "MsAi3yotmdA

Avoiding loss / theft

- Do not leave portable equipment unattended whilst travelling.
- Do not leave portable equipment unattended in hotel rooms, e.g. consider using hotel safes.
- Do not leave portable equipment unattended at customer or client sites.
- At home, equipment should be placed where it cannot be seen from outside, certainly away from windows and out of sight of casual visitors.
- Do not leave portable equipment unattended in vehicles. If it is unavoidable and you need to leave the equipment unattended for a very short time (e.g. when filling up with petrol), ensure the equipment is locked away out of sight.
- Ensure that if physical locking capabilities are available, these should be applied whenever the portable equipment is not in use, e.g. the use of security cables.
- Ensure that adequate physical protection should be applied to the equipment if it is to be stored at the user's home (locked cabinet).
- Ensure that the theft of portable computer equipment is immediately reported to the police and the Council's Financial Manager - Insurance & Loss Control at the earliest opportunity.
- Ensure that you are authorised to removal equipment from the council's premises.

Protecting Sensitive/Confidential Information

- All data on laptops remains the property of the Council.
- Always use any 'power on' password features as a simple deterrent to opportunistic usage.
- Ensure that no unauthorised people can gain access to the equipment. For example, do not lend the equipment to family or friends.
- ICT will ensure that all laptops and other types of personal computer are encrypted and verify that any encryption software is working properly.
- Follow any Council guidance on virus protection.
- Where possible restrict the sensitivity of information loaded onto laptops and similar portable computers. For instance only ever load the minimum information needed for that day.

  - Ensure information is regularly backed up and that old / no longer needed information is removed as over time (especially when equipment is shared amongst several employees) information can accumulate unnecessarily.

BEST PRACTICE

- When carried on the person, consider using a suitable carrying case that does not make it apparent that it contains a laptop.

1.5 TRAVELLING WITH LAPTOPS / PORTABLE COMPUTERS[6]

Persons who are issued with portable computers and who intend to travel for business purposes must be made aware of the information security issues and implement the appropriate safeguards to minimise the risks.

MANDATORY

- Store the equipment securely when not in use.
- Be mindful of where you are using the laptop as others may be able to look over your shoulder and view information.
- Never leave laptops left ‘on’ and unattended. Even if you password protect it, and unattended PC can be easily stolen.
- Users must take personal responsibility for the safety of their laptop and other portable computers.
- Where a laptop/portable PC is used by other people with differing access rights and privileges to the same of different systems as you then residual data and / or other information could remain on the PC which other users of the PC might not ordinarily have access to. Where possible, restrict the sensitivity of data which may be downloaded and stored on laptops. Ensure that you do not leave information on the laptop for others to see when they use it.
- Do not take laptops, tablet PCs and other ICT equipment that stores confidential or restricted information outside of the UK because they may be confiscated at the airport / border control. Also using them abroad is less secure than using them within the UK

[6] (ref: 010403 – 09.02.05 Security of equipment off-premises, 11.07.01 Mobile computing and communications)

Appendix A. A GUIDE TO INDIVIDUAL RESPONSIBILITES

This table shows were the primary responsibility for each section of this policy rests.

	ICT Services	Managers and Supervisors	All Employees	Finance Mgr – Treasury Mgt & Insurance
Introduction	✓	✓	✓	
Scope	✓	✓	✓	
Section 1 – Use of Portable ICT Equipment				
1.1 Backing up Data	✓		✓	
1.2 Issuing Portable Equipment	✓	✓	✓	
1.3 Insuring Laptops / Portables for use Domestically or Abroad				✓
1.4 Day to Day Use			✓	
1.5 Travelling with Laptops / Portable Computers			✓	

Appendix B. ICT EQUIPMENT AND POLICY ACCEPTANCE PROFORMA

ISSUE OF PORTABLE COMPUTING EQUIPMENT		
PLEASE COMPLETE IN BLOCK CAPITALS		
Directorate	Division:	Location:
Name:	Tel No:	E-mail Address:

Equipment Specification:

Make:

Model:

Serial Number:

SMBC Badge No.:

Accessories (tick/complete as necessary):

Batteries/Power Pack □

Battery Charger □

Power Cable □

External Mouse □

External Disk Drive/CD Unit □

Modem and Phone Socket Adaptor □

Carrying Case □

Instruction Book/Manual □

Printer and Cable □

Security Cable □

Other: □

Documents □

Corporate policy on the use of portable ICT equipment □

Confirmation of acceptance of policy and ICT Equipment

I confirm that by signing this form I have received the above equipment and have viewed the contents of the policy included above. I accept responsibility for the safekeeping of the equipment and contents of the portable computing facilities and agree to adhere to the Council's Information Security policies and guidelines in this respect.

Signed:	Date:

[Copy to be retained by the ICT Service Desk]