Hull Teaching Primary Care Trust

COMPUTER EQUIPMENT AWAY FROM WORKPLACE

CONTENTS

1. INTRODUCTION

Hull Primary Care Trust supplies computer equipment for use by PCT staff both in and away from the workplace. This Policy should be read in conjunction with the Home Working Policy.

Throughout this Policy the term 'computer equipment' refers to personal computers, laptops and tablets or any mobile computer equipment provided by the Trust.

2. AIM

The aim of this Policy is to support staff who use NHS computer equipment away from the workplace by ensuring staff are aware of computer security issues. In order to protect staff and others as well as NHS assets and systems, staff who use computer equipment at home must take appropriate security measures. The security issues covered in this Policy include the physical security of computer equipment, data confidentiality, and the security of NHS office systems and network.

Use of NHS computers and data resources must comply with the PCTs' legal obligations under the Data Protection Act 1998, Copyright, Designs and Patents Act (1988), Disability Discrimination Act (1995), Access to Health Records Act (1990) and other appropriate legislation.

3. SCOPE

This policy and procedure applies to all PCT employees irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership. All employees will be treated in a fair and equitable manner and reasonable adjustments will be made where appropriate (e.g. interpreter or signing provision, access arrangements, induction loop, etc.).

4. POLICY STATEMENTS

GENERAL

- All employees will be made aware of this Policy.

- The telephone helpline for IT users is available during office hours. However, you will need to bring the equipment to the IT Support Department for repair/upgrading. NHS computing systems are available during office hours but not necessarily out of hours.

- On terminating employment, NHS computer equipment, software, data, materials and information must be returned to the IT Department.

5. APPROPRIATE USAGE

- E-mail:

  Please note the following:

  - Person Identifiable data must not be sent off site via e-mail. See Appendix A for a definition of person identifiable data.

  - Internet e-mail services of any sort are not secure and should not be used to send Person Identifiable or other confidential information.

  - Staff must not use the automatic forward tool where the recipient will be via a commercial ISP (Internet Service Provider) such as Hotmail, Yahoo, etc.

  - Staff sending e-mail should be aware that it is not suited for confidential communications. Various systems are used for receiving e-mail and there is no guarantee that the addressee will be the only person to see the mail.

- To restrict the possibility of viruses being transmitted to NHS computers and network staff must not use their own computer for work-related activities unless anti-virus scanning software has been installed.

- *When you transfer files from your personal home computer to the office environment via floppy disk or USB STICK you must virus scan the "A: & USB drives" of your office computer using the virus scanning software. Information is available in Appendix B.*

- *When you remove equipment and data from NHS premises you are responsible for ensuring its safe transportation and storage as far as is reasonably practical. Equipment should be kept out of sight and not be left unattended at any time. Computer equipment must be transported in a secure, clean environment and must not be left in a vehicle overnight. You may be held liable if you do not take reasonable precautions.*

- You must take all reasonable steps to minimise the visibility of computer equipment from outside the home, and to secure windows and doors when the home is unoccupied.

- Any confidential paper document taken home must be stored in the most secure area of the home.

- Staff must ensure that if they are using a PCT computer equipment for mobile working, this must be set up by Hull IT engineers to allow synchronisation of user data with the network. This allows copies of folders to be transferred to the computer equipment when disconnecting from the network and then updates the server when reconnecting.

- The computer equipment must not be connected into any home network or allow it to be used to download any files/programs from anywhere, unless prior written agreement has been approved from the IM&T Manager and the computer equipment has been set up accordingly.

- Staff must not use their computer equipment for internet access via a modem, broadband or wireless connection unless they obtain prior written agreement from the IM&T Manager and the IT Engineers have set up the computer equipment accordingly.

- Staff must ensure that data is stored in compliance with the Records Management Guidance

- Staff must ensure that no confidential patient data is stored on their computer equipment. You must store copies of any documents containing patient data on a floppy disc or USB STICK, not the computer equipment hard drive. If your computer equipment does not have a floppy disk drive or you do not have a USB STICK, then it should not be used for personal identifiable data.

6. LEGAL LIABILITY

There is a legal requirement for the Chief Executive to report any computer crime involving accessing illegal material to the police. Users of the Internet are committing a criminal offence by downloading illegal material and the PCT would be required to involve the police if such materials were found on any of its computer equipment.

7. MISUSE OF THE POLICY

The PCT may instigate the disciplinary procedure if there is evidence to suggest that mobile working is being abused.

8. REVIEW DATE

This policy will be reviewed in partnership with the recognised trade union partners within 2 years of the date of implementation.

Author: Tracey Meyer
Title Head of IM/T
Date 3rd October 2006

Approved by:
Reviewed by:

Appendix A – Definitions

Person Identifiable Data

Person Identifiable Data is defined as any of the following items:

Surname, Forename, Initials, Address, Postcode, Date of Birth, Other Dates, Sex, NI Number, NHS Number, Hospital Number, Ethnic Group, Occupation, CHI, any registration number / identifier that is unique e.g. GP Practice registration, registration number (UKCC as was) etc
.

The Caldicott Report, "all items of information which related to an attribute of an individual should to be treated as potentially capable of identifying patients to a greater of lesser extent, and appropriately protected to safeguard confidentiality. Note should be taken of the degree of difficulty involved in actually identifying a specific individual, and this should be balanced against the purpose and usefulness of the specific items of information."