

Reference number G057
Approved by PCT Board
Date approved 27 March 2008
Last revised 19 February 2008
Review date 27 March 2012
Category General
Contact Director of Finance, Information, Estates and
Procurement
Who should read this All staff

Remote Access Policy

Title:	Remote Access Policy	
Purpose:	To provide secure and resilient remote access to the Trust's information systems	
Author/Responsibility of:	Author: Information Governance Team Leader; Responsibility: Trust Boards	
Applicable to:	All ICT Users working for Herefordshire Primary Care Trust (HPCT) or based at HPCT locations. All third party contractors working within HPCT. All third party personnel working within the HPCT.	
Scope:	Herefordshire Primary Care Trust.	
Revision History:	01 August 2005 – First Draft	
	01 September 2005 – Version 1.0	Approved
	19 February 2008 – Version 1.01	Director of Finance, Information and Performance changed to Director of Finance, Information, Estates and Procurement, Information Security Support Officer changed to Information Governance Team Leader. Minor amendments made to "Physical Protection" and "Access Controls". Addition of regular anti-virus and anti-spy-ware updates to mobile equipment to "Physical Protection". Addition of encryption of mobile devices used for confidential information to "Access Controls". Teleworking – express approval of Caldicott Guardian required to take personal/sensitive information home. Agreement by staff to ensure that Trust equipment is not used by unauthorised users or for unauthorised purposes added to "Teleworking (inc homeworking)"
	27 March 2008 – Version 1.1	Approved
Review Date	27 March 2012	
Action to be taken in event of breach of policy:	For members of staff actions will be taken in accordance with current HPCT Human Resources procedures. Any actions taken against third party contractors will be inline with the procedures agreed in the contractual agreements or information sharing protocols.	

1. Objective

To ensure information security when using mobile computing and teleworking facilities. This policy sets high level controls and is designed to ensure secure and resilient remote access to the Trust's information systems.

To maintain the security of organisational information processing facilities and information assets, when accessed by third parties.

2. Mobile computing and teleworking

2.1 Mobile information handling & computing

Mobile computing devices covered are: Laptop computers, Handheld (also known as palmtops, PDAs, pocket PCs). Many of the controls for computing devices also apply to use of paper based information.

Physical protection

In the majority of cases the use of mobile computing equipment takes place outside the organisation's premises. Where devices and paper information need to be used in a public environment, the following safeguards must be in place:-

- Users must take extra care to ensure that they are physically protected;
- Users are responsible for ensuring that mobile computing equipment or paper based information is never left unattended whilst in a public area;
- Devices and information must be transported out of public sight at all times;
- Devices owned by the organisation will be security marked;
- The use of security chains for laptops will be encouraged where possible;
- Users must take precautions to ensure confidential information either in paper form or on a computer screen cannot be seen by unauthorised individuals whilst working in public areas;
- All mobile devices must have anti-virus and anti-spy-ware components updated regularly in order to prevent the potential for a malicious or unauthorised mobile code attack;

-
- All mobile devices should be configured to synchronise data which has been processed on them, to the network at the end of a session, this will ensure that data is still available should the device be lost or stolen.

Access controls

Access to all mobile devices should be controlled through the requirement for a username and password to be entered; this will reduce the potential of unauthorised access to information. The Health Informatics Department will ensure all latest security patches are applied to a device's operating system. Mobile devices used for personal or sensitive data must be encrypted to the recommended NHS standard. Under no circumstances should confidential information be stored on unencrypted devices.

Connection to other networks

No organisational device will be connected to another organisation's network without express permission (the Procedure is documented in the full 'Mobile Computing, Home & off-site working (with information) policy'.

2.2 Teleworking (inc Homeworking)

Teleworking is the use of communication technology to enable staff to work remotely from a fixed location (including their home). Homeworking with either IT equipment or paper records will only be permitted for staff who have been approved for remote access. The following elements of policy are included:

- Physical security standards of the off-site facility (inc Home). Personal or sensitive information should not be taken home unless express approval has been gained from the Caldicott Guardian. Any information must be able to be locked away when not in use, with access only by the member of staff.
- Classifications of information to be accessed and/or retained off-site. Identifiable patient information and organisationally sensitive information must not be held on IT equipment not owned and managed by the organisation and should not be taken home without the express approval of the Caldicott Guardian.
- Agreement by staff members to prevent unauthorised access to information by relatives/friends/visitors and others.
- Agreement by staff members to prevent Trust equipment being used by unauthorised users or for unauthorised purposes.

-
- Backup and continuity procedures must be in place to ensure that information is not lost.
 - All remote access connections must be securely authenticated before the Trust information assets can be accessed.
 - Each request for remote access will be authorised by the Head of Department and approved by the Health Informatics Service. This approval will only take place if all of the security requirements have been met.
 - It is responsibility of departmental managers to inform the Health Informatics Service when an individual leaves the organisation or no longer requires Remote Access to the Trust's Systems.
 - Remote users will be restricted to the minimum services and functions necessary to carry out their role.
 - The Trust will ensure that all users of information systems, applications and the networks are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.
 - Security requirements must be addressed in 3rd party contract for all organisations that provide support and upgrade to information systems via a remote access solution.
 - Any 3rd party organisation that wishes to remotely access the Trust's Information Assets must sign up to the Trust's Information Sharing Protocol.
 - Regulatory and legislative requirements will be met

The 'Mobile information handling & computing policy' includes processes for authorisation, management and revocation of staff privileges to use mobile computing and teleworking facilities.

3. Security of third party access

3.1 Identification of risks from third party access

Risks vary dependant on the type of access required. Physical on-site access has different risks from those posed by off-site networked access. Risks from third party access are in effect the same as the risks for any user, however the nature of third parties removes the direct control over individuals that is present in a formal first party employment arrangement. Risks associated with third party access should be identified and assessed prior to entering into a business relationship with the third party. Following

identification of and assessment of risks, controls will be applied via contractual arrangement as below:-

3.2 Governance requirements in third party contracts.

Contractual arrangements with third parties will include agreement on the classification of information, the need for confidentiality control and how this will be applied. Where confidential information is to be (or could be) accessed, the organisation will require any supplier to have formal contractual confidentiality clauses with all employees accessing such data.

Two standard areas for inclusion are:

On-site access

Third parties with 'on-site' access will be required to wear 'visitor' identification badges (in addition to any organisational ID they may carry). Where there is a partner relationship (such as with a University), then a joint ID badge may suffice.

System access authorisation will be via the same process as any other user, but will identify the individual as a third party.

Off-site access

'Network' access for suppliers or partner organisations will be via approved NHSnet or N3 connection (adhering to NHSnet\N3 connection codes/policy). It is permissible for access to a system to be put into a third party's facilities by extension of an organisation's network, provided the network and the recipient's own network are kept separate (as per NHSnet policy – See

Other items that will be considered for inclusion:

- Methods for assessing whether assets have been compromised
- Controls over return/destruction of information
- Agreement on acceptable levels of data integrity and availability
- Liabilities of the parties to the agreement
- Legal responsibilities (Data Protection, Intellectual Property etc)
- The right to revoke agreement or access by any party in particular circumstances
- Protection against malicious software
- Arrangements for reporting and investigating potential breaches
- Involvement with additional subcontractors
- Authorisation and authentication processes for users

4. Implementation

This policy is supported by the following policies and procedures:

- User Access Control Policy (HIS003)
- Exchanges of Information Policy (HIS013)
- Confidentiality Code of Conduct (G037)
- Data Protection Policy
- Event Reporting, Control and Management Procedures
- Risk Assessment Procedure
- Incident Management Procedure

The Information Security Officer has direct responsibility for maintaining the Policy and providing advice and guidance on its implementation

All managers are directly responsible for implementing the Policy within their organisational areas, and for adherence by their staff.

Remote Access users are responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources and notify the Trust immediately of any security events (weaknesses and incidents) and breaches.

Signature

On behalf of the Herefordshire Primary Care Trust I certify that this document is the Remote Access Policy for the Herefordshire Primary Care Trust.

Name in Full:

Role:

Signature:

Date: