Information Technology Access Control Policy & Procedure

Version 1.0

Important: This document can only be considered valid when viewed on the PCT's intranet/U: Drive. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

Please note: This policy is approved subject to an Initial Equality Impact Assessment.

Name and Title of Author:	Damian O'Mullane – Senior IT Engineer
Name of Responsible Committee/Individual:	Partnership Consultation Negotiation Forum (P.C.N.F.)
Equality and Diversity Impact Assessment	Details to be added after assessment
Implementation Date:	04 March 2010
Review Date:	04 March 2012
Target Audience:	**All Staff including GPs and Non-Executive Director's.**

Contents

1 Introduction

1.1 This document defines the Access Control Policy for Hull Teaching Primary Care Trust (HTPCT). This policy and procedure should be read in conjunction with other policies and procedures referenced in section 18. The policy is required to support the Trust's other initiatives to enhance the role of Information Governance as prescribed in the Information Governance Toolkit module.

2 Purpose

2.1 The purpose of this Policy and Procedure is to support the Trust's IT security policies (as in section 18) and prevent unauthorised access to Trust information systems and network services. This document describes the procedure for the registration and de-registration of Trust staff accessing the network and information systems.

3 Scope

3.1 This Policy and Procedure applies to all employees of the PCT, any staff who are seconded to the PCT, contracted and agency staff and any other individual working on PCT premises including General Practitioners (GPs) and Non Executive Directors (NEDs).

3.2 This policy and procedure applies in particular to new starters, leavers and those changing role within the Trust.

4 Responsibilities

4.1 Chief Executive

4.1.1 The Chief Executive has overall responsibility for ensuring the security of access to the Trust network and other information systems.

4.2 Directors

4.2.1 Directors are responsible for ensuring that the appropriate staff are given access to the network and relevant information systems only when required.

4.3 Managers

4.3.1 Managers are responsible for ensuring that notification of all starters is made to Hull IT Servicedesk two weeks before access is requested, and notifications of leavers is made before their final leaving date.

4.4 Human Resources

4.4.1 Human Resources are responsible for providing the IT department with a list of leavers on a monthly basis.

4.5 Staff

4.5.1 All staff are responsible for the security of their username and password. Passwords should not be written down, shared or given out. All staff hold a responsibility to identify machines that are not in use to the IT department to ensure they are made secure.

4.5.2 All staff have a responsibility to lock any machine they are logged on to when it is not in use (e.g. when temporarily away from their desk).

5 Definitions

Lock - Computer systems that a user is logged on to but not temporarily using should be locked using Ctrl-Alt-Del

Leaver – An individual who will no longer be working for the Trust.

Ticket – An instruction of work to be followed and completed.

6 Equality and Diversity

6.1 The PCT is committed to:

- Eliminating discrimination and promoting equality and diversity in its policies, procedures and guidelines, and
- Designing and implementing services, policies and measures that meet the diverse needs of its population and workforce, ensuring that no individual or group is disadvantaged.

6.2 To ensure the above, this Policy has been Equality Impact Assessed.

6.3 Details of the assessment are available on the PCT's website or by calling the PCT on (01482) 344700.

7 NHS Constitution

7.1 The PCT is committed to:

- the achievement of the principles, values, rights, pledges and responsibilities detailed in the NHS Constitution, and
- ensuring they are taken account of in the production of its Policies, Procedures and Guidelines.

7.2 This Policy and Procedure supports the NHS Constitution through the duty to protect the confidentiality of personal information that is held unless to do so would put anyone at risk of significant harm (Section 3b).

8 New Users - Staff

8.1 Access to Trust managed information systems is controlled through a formal user registration process beginning with a formal notification from the new user's line manager, or in some cases from Human Resources.

8.2 Each user has a unique login username (e.g. gpquinn) so that users can be linked up to, and are accountable and can be made responsible for their actions. Only occasionally will there be a need for a group login i.e. training, but access rights are usually severely limited in these cases.

8.3 The level of authorised access should be the minimum which is required to effectively carry out the member of staff's daily duties and the level of access, including to other services must be specifically authorised by line management.

8.4 Any request for access must be made in writing (by email or hard copy) by the newcomer's line manager or by Human Resources. The request must state:

- The name of person making the request
- The job title of the newcomer and occupational work group (i.e. Administration etc.)
- The contact details (Workplace and telephone number)
- Start Date
- Services required. (Default services are: Email (including distribution lists), Microsoft Office, Internet access and U: Drive)

8.5 The new user request form can be found on the U: Drive under Corporate Templates and Forms, IT Folder.

9 New Users - IT Department

9.1 The new user registration procedure is as follows:

- Upon receiving the request in writing (by email or hard copy) from the Manager or HR, the request should be filed under 'profiles' in the ITS Servicedesk mailbox.

- The Servicedesk should then create a 'ticket' and pass requests for additional services from Infrastructure Team at Humber.

- The Servicedesk set up the new user and close the ticket. A test email is sent containing security guidance documents.

9.2 A new user will be set up on receipt of written notification but not made available (by issue of password) until the individuals start date. The new user will be advised of the user-id and password and then advised to change the password immediately.

9.3 The new user will be issued with security guidance documents via the test email. These documents include guidance on passwords, smartcards and safe computing.

9.4 The IT Servicedesk or the system administrator will maintain a record of all written requests in a folder, or an MS Outlook mailbox, for requests made via email. The requests will be retained for one year.

10 Change of User Requirements

10.1 Changes to user requirements will normally relate to an alteration to the applications used but may also involve network access. Requests must be in writing from the Line Manager and must be directed to the Hull IT Servicedesk. Changes will be made on receipt of a properly completed request, the same details as in 8.4 are required. Requests will be retained for one year.

11 Change of Password

11.1 Where a user has forgotten their password, the Servicedesk is authorised to issue a replacement. All such requests will be logged via the call logging process. The helpdesk will verify the person's identity by asking them to confirm details contained in their domain account.

12 Removal of Users - Staff

12.1 As soon as an individual leaves the employment of the Trust, all system access rights, must be revoked.

12.2 As part of the employee termination process, HR or line managers will inform the IT Servicedesk of all leavers and their date of leaving. This must be actioned as soon as possible after receiving notification of a leaver and no later than 2 days before the official termination date (wherever reasonably practicable). Please see the Notification of Leavers Policy and Procedure for further details.

12.3 All notification will be filed in a folder ('Leavers') by the Servicedesk. A list of 'leavers' will be provided by HR to the IT department on a monthly basis.

13 Removal of Users – IT Department

13.1 The de-registration procedure is as follows:

- Upon receiving the request in writing that the member of staff has left from the manager or HR, the request should be filed and retained for one year.
- The Servicedesk should raise a 'ticket' for the removal of all access rights with the Infrastructure Team.
- The Servicedesk should disable the user logon and email account and request the infrastructure team to remove the email account details within the address book. When confirmation of this is received, the Servicedesk will close the ticket.

13.2 All leavers should hand over current files within their workgroup, however, where this is not the case, as a precaution, the user account is moved into an organisational unit within 'Active Directory' and stored for three months as a back-up before complete removal.

14 Privilege Management

14.1 Special privileges are those allocated to the system administrator or service desk engineer, allowing access to sensitive areas (for example, passwords). The unnecessary allocation and use of special privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached. Privileged access must be authorised by the Head of Humber IT only.

14.2 The Head of Humber IT will maintain a master list of privileged accesses, which are in use, which will be checked and confirmed by the Information Security Manager on a three monthly basis. The list will identify all separate logons for each system and service.

14.3 The Head of Humber IT has right to suspend access for any individual under the guidance of Human Resources.

15 User Password Management

15.1 Password formats and general rules are controlled by inherited policy from Humber IT services, as they provide our infrastructure and its support.

The following rules for passwords apply:

- Previous passwords can only be re-used from the 6th change forward.
- The maximum password history is 60 days.
- The minimum password age is 1 day.
- The minimum password length is 6 characters and must include at least one number.

16 Review of Access Rights

16.1 The Head of Humber IT will instigate a review of all network access rights at least twice yearly, which is designed to positively confirm all users. Any lapsed or unwanted logons which are identified will be disabled immediately and will be deleted unless positively reconfirmed.

17 Monitoring Compliance with and Effectiveness of this Policy and Procedure

17.1 The effectiveness and compliance with this policy and procedure will be monitored via audits conducted twice a year.

18 Associated Documentation

- Notification of Leavers Procedure
- Mobile and Remote Working Policy
- Records Management Policy
- Email Policy

19 Review

19.1 This Policy and Procedure will be reviewed from two years from the date of implementation.

19.2 Minor amendments (such as changes in title) may be made prior to the formal review, details of which will be monitored/approved by the Associate Director of Corporate Affairs in consultation with the Equality and Diversity Co-ordinator and HR where relevant. Such amendments will be recorded in the Register and a new version of the PPG issued.