

Information System Remote Access Policy

Lead Executive/Senior Manager	Ward Priestman, Director of Informatics
Author with contact details	Neil Morgan, Information Security Manager, Ext 3588
Original Issue date	March 2006
State whether the policy is aimed Trustwide, Divisional or a local directorate level	Trustwide
If new policy, reason for development:	N/A
Date of this issue	October 2009
Approval Committee	
Policy consultation (including patient consultation):	
Policy applicable to (Identify by location and staff groups):	This policy is applicable to all members of staff who utilise the Trust Remote Access system.
Synopsis outlining policy aims:	<p>It is recognised that Remote Access is an increasingly valuable tool for employees of the Trust in connecting to the Trust's information resources when geographically removed from the primary hospital sites. As such, the Trust will support staff working in remote locations through the provision of a robust and secure access mechanism.</p> <p>This document details the requirements for remote access to Trust Information Systems and provides the required assurance through the provision of robust controls that:</p> <ul style="list-style-type: none"> – Provide secure remote access to the Trust information systems; – Preserve the Confidentiality, Integrity and Availability of Trust information and information systems; – Manage the risk of serious financial loss, loss of patient and public confidence or other serious adverse impact which may result from a failure in security; – Comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that the Trust is adequately protected under computer misuse legislation; – Facilitates staff access to Trust information resources and required systems from a remote location in a secure and safe manner.

Policy to be read In conjunction with:	Trust Information Security Policy Trust Antivirus Management Policy
Review Date	September 2011
Financial resource implications	Outline any financial implications of implementation of this policy e.g. resources required to train staff, resources for new equipment etc. and how these are going to be addressed?
Potential Risks of implementation	Connections of this nature may introduce risks that may have a serious adverse impact such as the following : <ul style="list-style-type: none"> – Unavailability of networks, systems or target information; – Degraded performance of remote connections; – Loss or corruption of sensitive data; – Loss or damage to equipment; – Breach of legislation or non-compliance with regulatory or ethical standards.
Outcome of E&D assessment	The policy has been screened and, with agreement from the Equality and Diversity lead within the Trust, a full impact assessment does /does not need (delete as appropriate) to be undertaken.

Document Change History (changes from previous issues of policy (if appropriate)) :

Issue Number	Page	Changes made with rationale and impact on practice	Date
V1.2		Due to the implementation of the Appgate Remote Access solution, policy re-written to address new requirements.	September 2009

6	APPENDICES TRAINING NEEDS ANALYSIS	9
---	---------------------------------------	---

1. INTRODUCTION/BACKGROUND

1.1 Scope

It is recognised that Remote Access is an increasingly valuable tool for employees of the Trust in connecting to the Trust's information resources when geographically removed from the primary hospital sites. As such, the Trust will support staff working in remote locations through the provision of a robust and secure access mechanism.

This document addresses all forms of remote working including:

- Mobile user e.g. staff working across sites or temporarily based at another location;
- Home workers e.g. IT Support, Corporate Managers, Clinicians etc;
- Any member of staff duly authorised.

1.2 Objectives

This document details the requirements for remote access to Trust Information Systems and provides the required assurance through the provision of robust controls that:

- Provide secure remote access to the Trust information systems;
- Preserve the Confidentiality, Integrity and Availability of Trust information and information systems;
- Manage the risk of serious financial loss, loss of patient and public confidence or other serious adverse impact which may result from a failure in security;
- Comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that the Trust is adequately protected under computer misuse legislation;
- Facilitates staff access to Trust information resources and required systems from a remote location in a secure and safe manner.

1.3 Definitions

1.3.1 Full Client

The Full Client is a computer that has all of the required information systems installed locally and accesses the data from the Trust Server.

1.3.2 Webmail

Webmail is a facility that enables staff to access their email via Internet Explorer without requiring the installation of the Outlook client.

1.3.3 Remote Desktop Procedure (RDP)

Remote Desktop is a function that enables you to securely connect to the Trust information systems and network drives via the Trust Terminal Server.

2. CONTENT OF POLICY

2.1 Access Mechanism

The Trust provides three different levels of remote access to staff via the Appgate Remote Access solution.

2.1.1 Webmail

The Webmail facility will allow staff to access their Trust email account remotely via the Internet Explorer application. Access to the Trust Webmail facility will be available to all Trust staff and may

be accessed, subject to the terms of this document, from both personal and Trust owned computers.

The printing of patient or proprietary data is strictly prohibited and may result in disciplinary action.

2.1.2 Full Client

The Full client will only be available upon Trust owned laptops or computers; this client will have the standard Trust build applied and will be managed by the Trust. All clinical systems will be available via this mechanism.

The printing of patient or proprietary data is strictly prohibited and may result in disciplinary action.

2.1.3 RDP Access

RDP Access will facilitate full access to Trust Information resources via the Terminal Server; the access mode will enable full access to all network resources including personal and departmental drives, Trust information systems and normal outlook access. RDP access will only be permitted via computers and/or laptops owned and managed by the Trust.

The printing of patient or proprietary data is strictly prohibited and may result in disciplinary action.

2.2 Authorisation of Remote Access

2.2.1 Webmail

If a member of staff requires access to the Webmail facility, appropriate authorisation must be provided by the appropriate Departmental Manager. Access will NOT be enabled without due authorisation.

2.2.2 Full Client

Access to Trust information systems via this mechanism must receive authorisation from either the Clinical Director or the Clinical Business Manager; this authorisation will also address the requirement for purchasing laptop and/or desktop for the member of staff.

2.2.3 RDP Access

Access to Trust information systems via RDP must receive authorisation from Director of Informatics and will only be facilitated in limited circumstances; RDP access may be enabled from the end users home laptop/computer.

2.3 Access Control

2.3.1 Risks Resulting from Remote Access

The Trust accepts that connections of this nature may introduce risks that may have a serious adverse impact as per the following examples (this list is not exhaustive):

- Unavailability of networks, systems or target information;
- Degraded performance of remote connections;
- Loss or corruption of sensitive data;
- Loss or damage to equipment;
- Breach of legislation or non-compliance with regulatory or ethical standards.

The Trust will implement appropriate controls to effectively manage the Risks resulting from the facilitation of remote access.

2.3.2 Authentication

Any remote access to Trust information systems will be conducted via the secure Appgate solution over a 256AES encrypted connection.

This will be further supported by the use of one-time authentication tokens issued directly to the mobile phone of the member of staff connecting remotely. This will require the provision of a mobile number by each member of staff requiring access; these numbers will be stored within the system only and no other copy will be retained.

2.3.3 Technical Controls

All computers used to access the Trust Remote Access system must comply with the following technical requirements:

- Minimum Windows Service Pack 2;
- Up to date antivirus software.

Failure to comply is a violation of this policy and will result in access being revoked.

2.3.4 Internet Connection

In order for a member of staff to be enabled with remote access, an appropriate internet connection must be in place at the residence in question. This connection **MUST** be purchased by either the staff member or by the appropriate Directorate; there are no special requirements for remote access and existing broadband connections are acceptable.

2.4 Remote Access Restrictions

2.4.1 Public Locations

Access to Trust information resources should not be conducted in any location that is deemed to be a public environment e.g. coffee shop, train station or any location where the screen may be visible to another person who does not have a legitimate purpose for viewing the data.

2.4.2 Private Locations

Remote access may be obtained from any location that has an internet connection and provides a secure location to connect without the risk of inadvertent disclosure of Trust data; such areas include at home, hotel rooms etc.

2.5 Terms and Conditions

All staff enabled with remote access are, at all times, bound by the terms of this document and by Trust policies and terms and conditions of employment.

2.6 Audit and Monitoring

2.6.1 Time and Date of Access

The Trust will maintain records all remote access sessions consisting of the time, date and duration of access.

2.6.2 Policy Compliance

The Trust will non-invasively scan each computer at the point of connection to ensure that the requirements as detailed within Section 2.3.3 are being adhered to and to ensure that a robust audit capability is maintained.

2.6.3 IP Address Monitoring

The Trust will record the IP address utilised to initiate remote connections in order ensure that legitimate access is maintained. The recording of this information will enable the Trust to ensure that non-legitimate access attempts are not being made and will enable the Trust to take appropriate action if identified.

2.6.4 Additional Monitoring

The Trust will conduct no additional monitoring unless stipulated within this document.

3. DUTIES AND RESPONSIBILITIES

3.1 Trust Senior Information Risk Owner (SIRO)

The Trust SIRO will be accountable for all information risks associated with the implementation of a remote access solution and will act as a focal point for the management of said risks.

3.2 Trust Information Security Manager

The Trust Information Security Manager will be responsible for ensuring that the remote access solution is deployed in a secure and robust manner in order to maintain the Confidentiality, Integrity and Availability of Trust information resources.

3.3 Staff

All staff are responsible for abiding by the requirements of this document and all associated Trust policies as identified within Section 5.

3.4 Policy Review

The Information Governance Steering Group will be responsible for identifying and assessing any requested changes to this policy. This will include the identification of any associated resource implication and to ensure the policy is updated officially and in accordance with Information Security requirements.

4. MONITORING EFFECTIVENESS

The production of weekly reports addressing the minimum requirements for connection stipulated within this document will be reviewed upon production. Any exceptions identified will be escalated to the Trust Director of Informatics and reported to the Information Governance Group.

5. REFERENCES

Information Security Policy

Email Policy

Internet Policy

Data Protection Policy

Information Governance Policy

Data Protection Act (1998)

ISO 27002: Code of Practice for Information Security Management

**APPENDIX (Please insert appropriate Appendix number in here)- Training Needs Analysis
for (Please insert name of policy in here)**

Please tick as appropriate

There is no specific training requirements- awareness for relevant staff required, disseminated via appropriate channels (Do not continue to complete this form-no formal training needs analysis required)	✓
There is specific training requirements for staff groups (Please complete the remainder of the form-formal training needs analysis required- link with learning and development department.	

Staff Group	✓ if appropriate outlining any exclusions within this staff group	Frequency	Suggested Delivery Method (traditional/ face to face e-learning/handout)	Does this need to be included in Trust wide mandatory learning programme for this staff group (✓ if yes)
Career Grade/Trust Grade Doctors (Consultants, speciality doctors, clinical fellows etc.)				
Training Grade Doctors				
Locum medical staff				
Registered Nursing Staff				
Clinical Bank Staff Registered				
Clinical Bank Staff Non Registered				
AHPs (Occupational Therapists, Speech & Language Therapists, Dieticians, Podiatrists, Physiotherapists)				
Additional Clinical Services (Nursing Assistants, Allied Health Professional Assistants, Lab Assistants, Support Worker, Radiology Assistants, Phlebotomists, Plaster Techs, Physiology Assistants)				
Healthcare Scientists (Qualified Laboratory staff, Qualified Mortuary Staff, Qualified Physiology Staff (Cardiology, Respiratory and Audiology), Rehab Engineers, Medical Technical Officers)				
Additional Professional Scientists and Technical (Pharmacists, Pharmacy Technicians, Theatre Practitioners/Team leaders, Biomedical Engineers, Optometrists, Orthoptists, Chaplains, MFU Technicians, Dental Hygienists, Audiology Technicians)				
Estates and Ancillary (Maintenance Staff, Estates Officers, Domestic, Laundry, Catering, Porters, House Keepers, Transport, Stores, Telephone Services)				
Admin & Clerical				

ADDITIONAL INFORMATION FOR CONSIDERATION (e.g. Source of Training Requirements)

--