Walton Centre

Remote working

Document History

Date	Version	Author	Changes
01/10/2004	1.0	A Cobain L Wyatt	
07/01/2005	1.1	L Wyatt	Update to requirements for access

Table of Contents

1. Introduction

Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of the Trust.

The Trust acknowledges that we must demonstrate to third parties our expertise in security technology and implementing it. To achieve this it is recognised that we must protect our own assets as well as the environment.

The aim of the Trust Security Policy, Security Standards and Work Instructions Manual is to maintain the confidentiality, integrity and availability of information stored, processed and communicated by and within the Trust. These standards, procedures and policies are used as part of the information security management system (ISMS) within the Trust.

The Trust will support staffs who, in appropriate circumstances, wish to undertake a part of their work either at home or from a remote location. As such, the Trust wishes to promote flexible working practices, reduce unnecessary travel and give staff more control over their working lives. This policy covers all aspects of working practice for members of staff undertaking work outside their conventional workplace.

This procedure outlines the method used for remote working.

2. Responsibilities Within This Standard

Particular responsibilities within the standard are defined as:-

Review and Maintenance	Information Security Officer
Approval	Information Security and Governance Group
Local adoption	Line managers (in scope)
Compliance	All staff and contractors (in scope)
Monitoring	Information Security Officer Information Security Auditor

3. Remote working procedures

This section outlines the control procedures in place for remote working.

- Remote working must be approved by the Head of IT/Information Security Officer.
- Connection will only be made to the Trust network secure broadband access.
- A single entry point will control access to the network, e.g. firewall and secure ID Token.
- Users must authenticate to the network, by using two-factor authentication
  - Secure Token across a broadband line
  - Relevant Trust network user account (User name and password)

3.1 Terms and Conditions

Employees must identify themselves to the network by using their own logon credentials.

Two-factor credentials must be kept confidential at all times.

Lost tokens must be reported immediately so accounts can be disabled, this would also need to be documented as a security incident.

Employees who are leaving the company must ensure that all equipment is returned to Systems Manager so accounts can be disabled on the last day of employment.

If an employee's contract is terminated, it is the responsibility of the Systems Manager to ensure the necessary accounts are disabled.

Any agreement on remote working is not permanent and may be brought to an end at any time by the member of staff or the Trust. An authorisation will be based on the needs of the Trust, the job, and the department. The authorisation is based on full, written agreement to the Trust's policy on remote working, see appendix 1 and completion of a satisfactory health

and safety risk assessment which must take into account all foreseeable risk arising from the work activity, and at the remote workplace, see appendix 3. The Trust will not give authorisation to staff to work remotely if they have not had approved appendices 1 and 3. Members of staff must comply with all the Trust rules, policies and practices and instructions whilst working remotely. Any failure to do so may result in approval to work remotely being revoked and/or disciplinary action.

4. Provision of Equipment

The Trust will not provide or maintain a home PC or broadband connection, but will provide the necessary additional equipment to enable remote connection to the Trust's network if necessary and required. This equipment could include:

- An active Token, synchronised to the network to provide once only passwords for secure login;

The Trust will set-up and test home equipment to ensure that Trust software is correctly installed and the connection to the Trust's network is functioning and secure. Supplies necessary to work at a remote site should be obtained during a work period in the conventional workplace.

Laptops will be provided on an exceptional basis and at the discretion of the relevant director/head of function or service/the postgraduate dean. Laptops are not primarily for home working but for staff who need to regularly move from one workplace to another in the course of their normal work.

The Trust is not liable or responsible for the support of home equipment except in respect of the equipment and software detailed above and directly relevant to remote access the Trust's systems.

The Trust monitors who logs into the network and can monitor which Internet and *NHSnet* sites are visited by any one user. Access to the remote access server is provided on the understanding that this is the case.

Any hardware or software provided by the Trust remains the property of the Trust and shall be returned at the end of the remote working arrangement. An equipment/software inventory will be completed by ISD for assigned Trust equipment to be used off-site.

Products, documents and other records used and/or developed while working remotely remain the property of and will be available to the Trust. This information is subject to Trust policies regarding confidentiality and access, including the Caldicott recommendations.

Trust owned software may not be duplicated. Staff working remotely using Trust software must adhere to the manufacturer's licensing agreements.

Each member of staff working remotely is responsible for protecting the integrity of copyrighted software, and following policies, procedures, and practices related to them to the same extent applicable in the conventional workplace. The member of staff must take all precautions necessary to avoid contamination of data for example by use of unauthorised software that may contain a computer virus.

The member of staff working remotely is responsible for setting up and maintaining an adequate workspace at the remote workplace and for ensuring that it is maintained to the same standards as apply to the conventional workplace.

Purchasing and maintenance of personal office furniture or equipment eg desks, filing cabinets, answering devices, etc, is the responsibility of the member of staff working remotely.

With reasonable notice and at mutually agreed times during working hours, the Trust will make on-site visits to remote workplaces to assess the health and safety risk (see appendix 3), or to inspect the remote workplace to ensure that it is sufficient for the equipment, or to check whether it is safe from hazards or to install or retrieve the Trust's equipment or property. Visits may be made by the Trust's designated health and safety officer, the line manager or anyone designated by the line manager.

5. Health and Safety

Most of the regulations under the Health and Safety at Work Act 1974 and all other current health and safety legislation, apply to staff working remotely as well as when working in their conventional workplace. Authorisation for remote working is subject to satisfactory completion of appendices 1 and 3.

The Trust will have the same responsibility for job-related accidents or injuries to the member of staff at the remote workplace that it has at the member of staff's conventional workplace.

The Trust is not responsible for any injury to any other person at the member of staff's remote workplace.

The member of staff is responsible for establishing and maintaining a designated, adequate workspace at the remote workplace. This space should be maintained to the same safety and other standards as are applicable in the conventional workplace. With reasonable notice and at mutually agreed times during working hours, the Trust may make visits to the home or remote location to assess health safety and welfare of the member of staff.

The member of staff is responsible for telephoning in to the conventional workplace at scheduled times agreed by prior arrangement with their line manager. This is a health and safety measure considered standard practice within remote working arrangements.

6. Reimbursement

The Trust will not reimburse staff for the use of any privately owned equipment.

Charges for calls made to the specified remote access server numbers will be reimbursed against completed expenses claim form with the appropriate paid
and itemised invoice. The member of staff should pay the standard broadband connection.

7. Confidentiality

As the *NHSnet* is a closed network and access from other networks is very strictly controlled, staff should be aware that the greatest risk to security is posed by those within the network, and not by outsiders. The *NHSnet* cannot protect systems from the actions, legitimate or otherwise, of other users. Therefore, all staff should be especially aware of the Trust's security and Internet and E-mail policies. Staff should also ensure that they are meeting the requirements of the Data Protection Acts 1984 and 1998, and at all times behave in accordance with UK law.

Staff working on Trust or associated organisations material/work must at all times take extreme care to ensure that confidentiality is maintained. Sensitive and confidential material

must not be taken out of the conventional workplace without prior approval by a member of staff's line manager.

8. Compliance

8.1 Responsibility

It is the responsibility of all users to ensure that they have read, understood and abide by this standard.

8.2 Review and Monitoring

The Walton Centre has in place routines to regularly audit compliance with this and other standards.

Appendix 1: APPROVAL FOR REMOTE WORKING

The member of staff/secondee named below has received express approval to work remotely and has read, understood and agrees to the conditions within the Trust's policy on remote working including those of the *NHSnet*.

Equipment being used

Description …….....

Assed Number ……..

Name of applicant ……..

Signature ……..

Date ……..

Line Manager ……..

Signature ……..

Date ……..

Head of IT/Information Security officer ……..

Signature ……..

Date …….

Valid until …….

An approved remote working application should be kept by the member of staff, their line manager with one copy for the personal file and one copy to IM&T.

APPENDIX 2:UNACCEPTABLE USE OF *NHSnet*

***NHSnet* may not be used for any of the following:**

The creation or transmission (other than for properly supervised and lawful clinical purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material

The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety

The creation or transmission of defamatory material

The transmission of material such that this infringes the copyright of another person

The transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks

Non-healthcare profit making activity that grossly abuses the service

Other activities that do not benefit patient care or that do not support the professional concerns of those providing that care, where those activities constitute gross abuse of the service

Gross abuse of the service by the unsolicited sending of inappropriate e-mail to large numbers of people, whether on *NHSnet* or on the Internet

Deliberate unauthorised access to facilities or services accessible via *NHSnet*

Deliberate activities with any of the following characteristics:

- Flagrant wasting of staff effort or networked resources, including time on end systems accessible via *NHSnet* and the effort of staff involved in the support of those systems;
- Corrupting or destroying other users' data;
- Violating the privacy of other users;
- Disrupting the work of other users;
- Using *NHSnet* in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
- Continuing to use an item of networking software or hardware after the NHS Information Authority - Telecommunications has requested that use cease because it is causing disruption to the correct functioning of *NHSnet;*
- Other misuse of *NHSnet* or networked resources, such as the introduction of "viruses";
- Where *NHSnet* is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of *NHSnet*.

Note that this list is not exhaustive, and will be updated in the light of experience.

If you are in doubt about whether you may use *NHSnet* for a particular purpose, you should seek advice from your NHS Information Authority - Telecommunications local office.

It is not permitted to provide access to *NHSnet* by third parties without the prior agreement of the NHS Information Authority - Telecommunications.

Source: NHS Information Authority
May 1999

APPENDIX 3: HEALTH AND SAFETY Responsibilities

The Trust cannot accept the responsibility for the health and safety of a remote working environment

- If the remote site is, another Trust or facility providing a service to The Walton Centre the Health and Safety of the user will fall under the remote site's health and Safety guidelines.

- If the remote users is working from home it will be the individual's responsibility to ensue that they conduct any work for the Trust in a safe and practical manor as they world if situated in an office environment within The Walton Centre.

The following list is a guide that the Trust recommends that a remote user should follow when working from home.

WORKPLACE ENVIRONMENT

1. Try to work in an environment were temperature, noise ventilation and lighting levels are adequate for maintaining your normal level of job performance.

2. All stairs with four or more steps equipped with handrails.

3. You have circuit breakers and/or fuses in the electrical panel labelled as to intended service.

4. Any circuit breakers clearly indicate if they are in the open or closed position. If they are not could one be put in place?

5. Do you have all electrical equipment free of recognised hazards that would cause physical harm (frayed wires, bare conductors, loose wires, flexible wires running through walls, exposed wires to the ceiling)?

6. Dose your homes electrical system permit the grounding of electrical equipment?

7. Is the environment you have chosen, free of obstruction to permit visibility and movement?

8. If you have, any filing cabinets and storage closets are they arranged so drawers and doors do not open into walkways.

9. Make sure that any chairs, which will be used for work purposes, have no loose casters (wheels) and the rungs and legs of the chairs are sturdy. If posable use adjustable one to help with posture when working for any prolonged period of time.

10. Tidy all phone lines, electrical cords, and extension wires so that they secured under a desk or alongside a baseboard?

11. Try to keep office space neat, clean and free from clutter that could become a hazard.

12. Try to keep any floor surfaces clean, dry, level and free of worn or frayed seams in your chosen working environment and carpets are well secured to the floor and free of frayed or worn seams?

13. You have enough lighting for reading

14. Try to have a basic first aid kit in your home.

15. If you do not have one fit a smoke alarm

16. Try to use an area of the home were you can set up your computer so that the monitor and keyboard are in the correct position for a combatable and safe working area with plenty of space.

17. Set the computer up so that you can easily read the text on the screen.

18. Try to use a document holder.

19. Make sure you have enough legroom at your desk or chosen working area.

20. Try to chose a work area

The Trust will however take responsibility for equipment that it provides to a remote user and will ensure that it is in full working order when handed over to the user. The Trust will also maintain the equipment while the remote user is under the employment of The Walton Centre.

Once the period of remote, working has ended or the remote user has cessed, their employment with The Walton Centre all equipment must be returned to The Walton Centre.