London's global university

SLMS IDHS Remote Working Procedures and Approval

Document information	
Document name	SLMS-IG21 Remote Working Procedures and Approval
Author	Shane Murphy
Issue date	02/08/2013
Approved by	Chair of SLMS IGSG
Next review	Three years

Document history		
Version	**Date**	**Summary of change**
0.1	02/02/2013	First draft for discussion
1.0	02/08/2013	Approved by Chair of SLMS IGSG

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 SLMS.

SLMS 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 and work within the requirements of the Information Governance Toolkit.

The aim of the SLMS and associated Policies, Standard Operating Procedures, Local Security Guidance and Work Instructions is to maintain the confidentiality, integrity and availability of information stored, processed and communicated by and within SLMS. These standards, procedures and policies are to be considered as SLMS's holistic approach to Information Governance.

SLMS 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, SLMS promotes 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

Review and maintenance	IG Lead and IG officer
Approval	Information Governance Steering Group
Local Adoption	Local managers and staff
Compliance	All staff, contractors and relevant third parties
Monitoring	IG Lead and Head of Information Security

3. Remote Working Procedures

This section outlines the controls required for remote working:

- The Head of information Security will approve remote working requests;
- Connection will only be made to IDHS through the SLMS secure network;
- Connection will only be made through two factor authentication, using a secure ID token and UCL network user account, via the UCL firewall

3.1 Terms and Conditions

Users 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.

Users who are leaving SLMS must ensure that all equipment is returned to their Line Manager, so that accounts can be disabled on the last day of employment.

If a User's contract is terminated, it is the responsibility of the Line 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 SLMS. An authorisation will be based on the needs of SLMS, the job, and business requirements. The authorisation is based on full, written agreement to the SLMS policy on remote working, see appendix 1 and completion of a satisfactory health and safety risk assessment. The risk assessment should take account of all foreseeable risk rising from the work activity and the place of work.

Completion of appendices 1 and 3 are a prerequisite for remote working approval. Users must comply with all applicable SLMS terms and conditions of employment, rules, policies, practices, procedures, work instructions and the reasonable instructions of management. Failure to do so may result in the withdrawal of remote access facilities and possible disciplinary action.

4. Provision of Equipment

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

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

SLMS will set-up and test home equipment to ensure that SLMS software is correctly installed and the connection to the SLMS'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 are provided on an exceptional basis and at the discretion of the relevant director/head of service. 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.

SLMS 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 SLMS's systems.

SLMS monitors who logs into the network and can monitor which Internet 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 SLMS remains the property of the SLMS and shall be returned at the end of the remote working arrangement.

An equipment/software inventory will be completed by ISD for assigned SLMS 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 SLMS. This information is subject to SLMS policies regarding confidentiality and access. Researchers, in particular, processing personal data are expected to comply with the Caldicott Principles.

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

Each user 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. Each user must take all precautions necessary to prevent data corruption, for example by use of unauthorised software that may contain a computer virus.

Each user 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 e.g. 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, SLMS 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 SLMS's equipment or property. Visits may be made by the SLMS's designated health and safety officer, the line manager or anyone designated by the line manager.

5. Health & Safety

Most of the regulations under the Health and Safety at Work Act 1974 and all other current health and safety legislation, apply to users 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.

SLMS will have the same responsibility for job-related accidents or injuries to Users at the remote workplace that it has at the User's conventional workplace.

SLMS is not responsible for any injury to any other person at the User’s remote workplace.

The User 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 SLMS may make visits to the home or remote location to assess health safety and welfare of the User.

The User 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 Users 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 User should pay the standard broadband connection.

7. Confidentiality

The IDHS facility is a controlled and secure IT environment. Therefore, all Users should aware of the SLMS local information governance, security, Internet and E-mail guidance materials, policies, processes, procedures and work instructions. Staff should also ensure that they are meeting the requirements of the Data Protection Act 1998, and at all times behave in accordance with UK law.

Staff working on NHS or associated organisations material/work must at all times take extreme care to ensure that confidentiality is maintained. Personal and Sensitive data 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 comply with the requirements of these procedures.

8.2 **Review and Monitoring**

IGSG will be responsible for the annual review of this document. The IG Lead will have responsibility for monitoring compliance with this procedure.

Appendix 1: Approval for Remote Working

The user identified below has received approval to work remotely and has read, understood and agrees to the conditions within the SLMS policy on remote working including those for use of the IDHS.

Equipment issued	
Description	
Asset Number(s)	
Name of Applicant (BLOCK CAPITALS)	
Signature	
Date (dd/mm/yy)	
Name of Line Manager (BLOCK CAPITALS)	
Signature	
Date (dd/mm/yy)	
Head of Information Security (BLOCK CAPITALS)	
Signature	
Date (dd/mm/yy)	
Valid until (dd/mm/yy)	

A record of this form should be retained by HR, Head of Information Security, Line Manager and the User

Appendix 2: Unacceptable use of IDHS

IDHS may not be used for any of the following:

The creation or transmission, or any other form of processing as defined by the Data Protection Act 1998, that is detrimental to the legitimate rights of individuals or likely to cause annoyance, inconvenience or needless anxiety. For the avoidance of doubt this includes but is not limited to the processing of racist, pornographic, sexist or terrorist materials.

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.

Deliberate unauthorised access to facilities or services accessible via IDHS

Deliberate activities with any of the following characteristics:

Flagrant wasting of staff effort or networked resources, through inappropriate and unauthorised use of IDHS facilities including but not limited to the following:

- Corrupting or destroying other users' data;
- Violating the consent, or wishes of data subjects in respect of processing personal or sensitive data;
- Violating the privacy of other users;
- Disrupting the work of other users;
- Using IDHS 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 AISC Information Security Manager has requested that use cease because it is causing disruption to the correct functioning of IDHS;
- Other misuse of IDHS or networked resources, such as the introduction of "viruses";
- Where IDHS is being used to transfer data to another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of IDHS.

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 IDHS for a particular purpose, you should seek advice from AISC Information Security Manager.

It is not permitted to provide access to IDHS by third parties without the prior agreement of AISC Information Security Manager.

Appendix 3: Health & Safety Responsibilities

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

• If the remote site is, a NHS Trust or facility providing a service to SLMS the Health and Safety of the user will fall under the remote site's Health and Safety guidelines.

• If the remote user is working from home it will be the individual's responsibility to ensure that they conduct any work for SLMS in a safe and practical manor as they world if situated in an office environment within SLMS.

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

WORKPLACE ENVIRONMENT

1. Users should work in an environment where temperature, noise, ventilation and lighting levels are adequate for maintaining your normal level of job performance.

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

3. You have circuit breakers and/or fuses installed in the relevant domestic fuse box and all electrical work has been carried out in accordance with IET Wiring Regulations and BS 7671.

4. Any circuit breakers clearly indicate if they are in the open or closed position. If they are not could this be rectified? Any socket-outlet not having RCD protection needs to be specifically labelled or otherwise suitably identified to indicate its intended use, such as 'freezer only'. Surge Protection Devices should be considered when using IT equipment to prevent power spikes from damaging the equipment.

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

6. Does 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?

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. Consider the use of adjustable chairs 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 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, foot rest, wrist support to avoid potential posture issues.

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

20. Ensure that your house insurance is adequate to cover the use of IT equipment in the home and that recommended locks and other domestic security devices meet insurance standards.

21. Do not leave IT equipment packing materials outside your house or flat – they are a calling card for potential thieves.

22. Do not work next to a ground floor open window and leave the IT equipment unattended.

23. Secure the IT equipment after use and do not allow other family members to use the IT equipment.

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 equipment whilst the user is working for the SLMS.

Once the period of remote working has concluded or the user is no longer employed or providing services for the SLMS the equipment must be returned to SLMS.