1. **Document Information**	
Document Name	SLMS-IG21 Remote Access Policy
Author	Shane Murphy
Issue Date	2/08/2013
Approved By	Chair of the SLMS IGSG
Next review	Three years

2. **Document History**		
Version	**Date**	**Summary of change**
0.1	19/02/2013	First draft for discussion
1.0	02/08/2013	Approved by the Chair of the SLMS IGSG

Aim:	To mitigate associated risks of remote working to an acceptable level within SLMS. The provision of best practice working procedures to ensure that staff work remotely in a safe and secure manner, thereby protecting personal and sensitive data.

Scope:	This policy covers all types of remote access, whether fixed or 'roving' including: Travelling users (e.g. Staff working across sites or are temporarily based at other locations) Home workers (e.g. IT support, Corporate Managers, IT development staff, researchers) Non SLMS staff (e.g. contractors and other 3rd party organisations)

Associated documentation:	Legal Framework: The Data Protection Act (1998), Copyright Designs & Patents Act (1988), Computer Misuse Act (1990), Health & Safety at Work Act (1974), Human Rights Act (1998) Regulatory: NHS CfH Information Governance Toolkit Version 10. Policies: Information Security Policy; Data Protection Policy; SLMS Information Governance Policy; email]

Review and consultation process:	Annually from review date above. Information Governance Steering Group to oversee process
Responsibility for Implementation & Training:	Day to day responsibility for implementation: IT for SLMS Head of Infrastructure Day to day responsibility for training: IG Lead

What is Remote Access?
Remote Access refers to any technology that enables you to connect users in geographically dispersed locations. This access is typically over dial-up or wireless connection.

Purpose of Policy
Remote access by SLMS staff is a method of accessing files and systems that is becoming more common in SLMS. Often, critical business processes such as IDHS (identifiable Data Handling Solution) rely on easy and reliable access to corporate information systems. In practice, the benefits of securing remote access are considerable – business can be conducted remotely with confidence and sensitive corporate information remains confidential. This document sets out the policy for remote access and includes a set of common controls, which can be applied to reduce the risks associated with a remote access service.

Willful or negligent disregard of this policy will be investigated and may be treated as a disciplinary offence.

Scope
This policy covers all types of remote access, whether fixed or 'roving' including:
Travelling users (e.g. Staff working across sites or are temporarily based at other locations)
Home workers (e.g. IT support, Corporate Managers, IT development staff, Researchers)
Non SLMS staff (e.g.contractors and other 3rd party organisations)

Objectives
The objectives of the SLMS's policy on remote access by staff are:
To provide secure and resilient remote access to the SLMS's information systems.
To preserve the integrity, availability and confidentiality of the SLMS's information and information systems.
To manage the risk of serious financial loss, loss of client confidence or other serious business impact which may result from a failure in security.
To comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that the SLMS is adequately protected under computer misuse legislation.

Principles
In providing remote access to staff, the following high-level principles will be applied:
The SIRO (Senior Information Risk Owner) will be appointed to have overall responsibility for each remote access connection to ensure that the SLMS's policy and standards are applied.
A formal risk analysis process will be conducted for each application to which remote access is granted to assess risks and identify controls needed to reduce risks to an acceptable level.
Remote users will be restricted to the minimum services and functions necessary to carry out their role.

Responsibilities
The SLMS SEG Board is ultimately responsible for ensuring that remote access by staff is managed securely.
The Information Governance Steering Group will maintain policy, standards and procedures for remote access to ensure that risks are identified and appropriate controls implemented to reduce those risks.
The SIRO is responsible for providing clear authorisation for all remote access users and the level of access provided.
The Information Governance Steering Group is responsible for confirming whether remote access to business applications and systems is permitted.
The Head of Information Security will ensure that user profiles and logical access controls are implemented in accordance with agreed access levels.
The IT for SLMS Head of Infrastructure will provide assistance on implementing controls.
All remote access users are responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources, notify the SLMS immediately of any security incidents and breaches.
Users must return all relevant equipment on termination of the connection.
Internal auditors are responsible for assessing risks and ensuring that controls are being applied effectively.

Risks
The SLMS recognises that by providing staff with remote access to information systems, risks are introduced that may result in serious business impact, for example:
unavailability of network, systems or target information
degraded performance of remote connections
loss or corruption of sensitive data
breach of confidentiality
loss of or damage to equipment
breach of legislation or non-compliance with regulatory or ethical standards.

Security Architecture
The security architecture is typically integrated into the existing SLMS network and is dependent on the IT services that are offered through the network infrastructure. Typical services include:

Password authentication, authorisation, and accounting
Strong authentication
Security monitoring by unified threat management and intrusion detection systems

Security Technologies
To ensure the most comprehensive level of protection possible, every network should include security components that address the following five aspects of network security.

User Identity
All remote users must be registered and authorised by the Head of Information Security. User identity will be confirmed by strong authentication and User ID and password authentication. The IT for SLMS Head of Infrastructure is responsible for ensuring a log is kept of all user remote access.

Perimeter Security
The IT for SLMS Head of Infrastructure will be responsible for ensuring perimeter security devices are in place and operating properly. Perimeter security solutions control access to critical network applications, data, and services so that only legitimate users and information can pass through the network. Routers and switches handle this access control with access control lists and by dedicated firewall appliances. Remote Access Systems with strong authentication software control remote dial in users to the network. A firewall provides a barrier to traffic crossing a network's "perimeter" and permits only authorised traffic to pass, according to a predefined security policy. Complementary tools, including virus scanners and content filters, also help control network perimeters. Firewalls are generally the first security products that organisations deploy to improve their security postures.

Secure Connectivity
The SLMS will protect confidential information from eavesdropping or tampering during transmission.

Security Monitoring
Network vulnerability scanners will be used to identify areas of weakness, and intrusion detection systems to monitor and reactively respond to security events as they occur.

Remote diagnostic services and 3rd parties
Suppliers of central systems/software expect to have dial up access to such systems on request to investigate/fix faults. The SLMS will permit such access subject to it being initiated by the computer system and all activity monitored.

Each supplier or SLMS user requiring remote access will be required to commit to maintaining confidentiality of data and information and only using qualified representatives.

Each request for dial up access will be authorised by approved ISD staff, who will only make the connection when satisfied of the need. The connection will be physically broken when the fault is fixed/supplier ends his session.

User Responsibilities, Awareness & Training
The SLMS 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. Irresponsible or improper actions may result in disciplinary action(s).

System Change Control
All changes to systems must be recorded on a Change Request form and authorised via UCL SCP process and CAB approval if necessary.

Reporting Security Incidents & Weaknesses
All security weaknesses and incidents must be reported to the Information Governance Steering Group through the UCL Computer Security Team
http://www.ucl.ac.uk/cert/reporting.html

Guidelines and training
IT for SLMS Head of Infrastructure and IG Lead will produce written guidance and training materials for all remote access users.

Validity of this Policy
This policy should be reviewed annually under the authority of the Senior Information Risk Owner. Associated information governance and security standards should be subject to an on going development and review programme.