Date user added	
Training requested	
Processed by	
Date user amended	

Internal IT use only

SCI Gateway HMP user account request form

v1.2 28/05/2012

This form must be completed for all new HMP user account requests for the SCI Gateway application.

Full Name	
Role / Job title	
HMP Name	
HMP Code	
Email address	
Contact telephone	
Name of first school attended **(in case password reset requested)**	

Please now read and sign the "NHS Greater Glasgow and Clyde Security Policy" section overleaf and ensure Health Centre Manager completes and signs below.

Health Centre Manager:

Health Centre Manager Name	
HMP Code	
Signature	
Date	

Return Form to

Fax: 0141 278 4770	**Email:** GG-UHB.GPFacilitatorTeam@nhs.net	**Mail:** IT Mentoring Team IT Dept Admin Building Gartnavel Royal Hospital 1055 Great Western Road Glasgow G12 0XH

NHS Greater Glasgow & Clyde Security Policy

Staff must keep in mind, that in the course of their employment, they are likely to see or hear information which may be of a sensitive nature. Protection of data about individuals is a requirement of the law.

The Data Protection Act 1998 lays down that:

- Data shall be obtained and processed fairly and lawfully;
- Data shall be held only for specific purposes and not used or disclosed in any way incompatible with these purposes.

All persons that process data on a computer, or use information, have an obligation to see that it is not passed on to any unauthorised person or organisation. This means, amongst other things, that printouts must be treated carefully and that staff must not disclose personal information in any way other than that which is required for the discharge of their duties to NHS Scotland.

It is vital that all staff understand their responsibility to treat as confidential, information which may be available to them, or obtained by them, or which may be derived whilst in the employ of, or contracted to, NHS Greater Glasgow & Clyde.

In the event of a breach of security arising, any member of staff responsible for, or who contributes towards the breach, may be subject to disciplinary action, which in serious cases can include dismissal. In certain circumstances this could result in prosecution.

Staffs are further reminded that they must never disclose network passwords to any other individual, thereby allowing unauthorised access to confidential information.

Security Devices, Passwords and User ID codes

I will ensure that any security devices, passwords and user IDs allocated to me for use with the Clinical Applications are kept confidential and secure, and not passed to any other person whether or not an employee of the hospital or practice. I further understand that I am responsible for any transactions carried out under my personal password and code.

Data Protection

I acknowledge that Data Protection legislation governs all information gathered or accessed by me. I understand that I may not extract subject identifiable data and hold it on any system not registered in accordance with the appropriate act.

I have read and understood the published IT security policies listed above and I agree to abide by them. I understand information on Clinical Applications is to be accessed **only** on a need to know basis.

Signature		**Date**	