



# INFORMATION TECHNOLOGY SECURITY POLICY

|                      |                     |
|----------------------|---------------------|
| Author               | IT Security Manager |
| Responsible Director | Director of eHealth |
| Approved By          | IG Steering Group   |
| Data Approved        | September 15        |
| Date for Review      | November 17         |
| Version              | 2.4                 |
| Replaces version     | 2.3                 |

### Consultation and Distribution Record

|                                     |                                                       |
|-------------------------------------|-------------------------------------------------------|
| Contributing Authors                | IT Security Manager<br>Information Governance Manager |
| Consultation Process / Stakeholders | Information Governance Steering Group                 |
| Distribution                        | All Staff                                             |

### Change Record

| Date   | Author  | Change                             | Version No |
|--------|---------|------------------------------------|------------|
| Mar 17 | I Brown | Change Control added               | 2.4        |
| Mar 17 | I Brown | Change wording from HIT to eHealth | 2.4        |
|        |         |                                    |            |
|        |         |                                    |            |
|        |         |                                    |            |
|        |         |                                    |            |
|        |         |                                    |            |

### Contents

|      |                                                  |   |
|------|--------------------------------------------------|---|
| 1.0  | Introduction .....                               | 3 |
| 2.0  | Scope.....                                       | 4 |
| 3.0  | Roles and Responsibilities .....                 | 4 |
| 3.1  | Role of Directors and Heads of Departments ..... | 4 |
| 3.2  | Role of Staff .....                              | 4 |
| 4.0  | New IT Facilities /Applications .....            | 4 |
| 5.0  | Access to IT Systems.....                        | 5 |
| 6.0  | Use of IT Systems.....                           | 5 |
| 7.0  | Auditing of .....                                | 5 |
| 8.0  | Procedures.....                                  | 6 |
| 9.0  | Copyright.....                                   | 6 |
| 10.0 | Policy Review.....                               | 6 |
| 11.0 | Communication & Implementation .....             | 6 |
| 12.0 | Further Advice .....                             | 6 |

## **1.0 Introduction**

The purpose of information security is to safeguard the Organisation's information within a secure environment and where appropriate, to share that information without compromising its confidentiality. Information Security Management is critical to the business needs of NHS Greater Glasgow & Clyde (NHSGGC).

The objective of information security is to ensure the confidentiality, integrity and availability of information, whilst minimizing the risk of loss, through the implementation of standards, controls and procedures, which support this policy.

### Associated Legislation:

- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Data Protection Act 1998•
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002
- Human Rights Act (2000)
- Privacy and Electronic Communication (EC Directive) Regulations 2003
- RIP Act 2000
- RIP(S) Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

### Associated Policies and Standards:

- ISO/IEC 27005:2005
- NHSScotland Caldicott Guardian's Principles into Practice – Nov 2010
- NHS Code of Practice: Protecting Patient Confidentiality
- NHSiS IT Security Manual

Having read, understood and accepting to be bound by the terms of this policy, and given a valid business reason, the reader may apply for access to the NHSGGC computer network and to applications which they require to use.

Access forms are available on StaffNet (NHSGGC Intranet).

## **2.0 Scope**

This policy applies to all staff employed by NHSGGC. It also applies to contractors, partnership organisations and visitors not employed by NHSGGC but engaged to work with, or who have access to, information systems and applications.

Additional policies and guidance documents are provided to address specific areas of IT Security.

## **3.0 Roles and Responsibilities**

### **3.1 Role of Directors and Heads of Departments**

Directors and Heads of Departments are responsible for ensuring that staff within their own directorates and departments work in a manner consistent with the principles outlined in the Policy.

### **3.2 Role of Staff**

It is the responsibility of all staff to ensure they have read and understood this Policy and to ensure high standards of confidentiality are met.

Staff must take ownership of this and other related policies and support their aims. This applies to all staff regardless of their contractual status within the organisation.

Specifically staff must:

- Always ensure a password protected screensaver is activated (this is done by using the  +L keys) or log off when leaving a PC;
- Only view information that is relevant to the work that they are performing. Viewing information which is not pertinent to their work is a breach of several UK laws. (It is not permitted to view the records of a patient for whose care they are not party to);
- Never disclose their passwords – even to IT Support. Many computer users have “Tap & PIN” to logon using Improvata One-Sign (Single Sign On). The PIN must never be disclosed;
- Never use somebody else’s userid and password; to do so is a breach of the Computer Misuse Act. Using someone else’s ID Card and PIN is the same as using their userid and password.

## **4.0 New IT Facilities /Applications**

The procurement of IT facilities may only be undertaken with the prior approval of the eHealth Directorate.

Staff introducing new IT facilities and applications (i.e. ‘systems’) must ensure that the applications, their use and management are compliant with the requirements of the NHS Scotland IT Security Policy and Manuals. The Policy and manuals can be found at: <http://www.security.scot.nhs.uk/>.

## **5.0 Access to IT Systems**

Staff must fully understand that all systems and services are provided as business tools and that there is no individual right of privacy when accessing these services.

Very limited trials are underway to permit restricted use of personal equipment to NHSGGC IT facilities. Outwith these trials Personal Equipment must not be connected to any NHSGGC computer or network.

Only authorised persons may access IT systems. Access must be restricted to information required for the authorised person's job function (i.e., on a need to know basis).

There are very many situations where PCs are shared, particularly in wards. To reduce the time to access applications there are currently many Generic network accounts (logons) where the passwords are shared, however no home or shared drive access will be permitted from these accounts, their sole purpose being to facilitate faster access to applications such as TrakCare and Clinical Portal. The end user will log onto each application using their own userid and password. This arrangement ensures controlled access and auditability of systems.

Technology changes are being rolled out that enable fast access to the network and applications and remove the need for generic network accounts.

## **6.0 Use of IT Systems**

Users will be supported in their use of information systems, they may however be held accountable for their actions.

If inappropriate use of any NHSGGC computer is known or suspected, then investigations will be instigated, either under the direction of H.R., by the police or other regulatory body as appropriate.

If managers believe that there is cause to initiate an investigation then they must contact a senior member of H.R. in the first instance. Please also refer to the Board's Data Breach Policy.

Investigations will be undertaken by IT/IG staff once instructions to do so have been given by an appropriate senior H.R. manager.

## **7.0 Auditing of IT Systems**

Evidence of who has viewed / entered / changed data in an application (e.g. TrakCare or Clinical Portal) is contained within the audit trail. The audit trail will record the ID of the person who was logged in and note which data the person viewed / entered / changed.

The audit log provides irrefutable evidence of the account that was used to perform the action and is effectively the user's signature. Where HR

investigate cases of potential inappropriate access, the audit log may be provided by the IT Department as evidence.

## **8.0 Procedures**

It is the policy of NHSGGC to ensure that:

- Information will be protected and controlled against unauthorised access or misuse;
- Confidentiality of information will be assured<sup>1</sup>
- Integrity of information will be maintained; <sup>2</sup>
- Business continuity planning and risk assessment processes will be maintained;
- Regulatory, contractual and legal obligations will be complied with;<sup>3</sup>
- Information security training will be provided to staff;
- Information assets will be registered, classified and protected;
- All health board owned computers will have centrally controlled, automatically updated anti-virus software installed. Such controls shall ensure that there can be no user intervention;
- Cryptographic technologies will be employed as appropriate;
- Physical, logical and communications security will be monitored and maintained;
- Operational procedures, protocols and policies will be regularly reviewed and maintained;

If using any mobile computing or removable storage media, then the Mobile Devices and Media Policy shall apply.

## **9.0 Copyright**

Downloading, copying or re-using any third party copyright material from the internet must be in compliance with both the Copyright, Designs and Patents Act 1988, and the NHS Scotland Copy Policy 2011. For more information see the guidance provided on the Copyright page on StaffNet.

## **10.0 Policy Review**

This policy will be reviewed every two years unless the introduction of any new or amended relevant legislation warrants an earlier review.

## **11.0 Communication & Implementation**

This Policy will be communicated through the Information Governance and IT Security Framework.

## **12.0 Further Advice**

For further advice on this Policy please contact the IT Compliance Manager.  
Tel: 0141278 4728 Email: [Stephen.harris@ggc.scot.nhs.uk](mailto:Stephen.harris@ggc.scot.nhs.uk)

**Notes:**

1 Valuable information will be protected against unauthorised access and disclosure.

2 Safeguards will be created to protect against unauthorised modification or destruction of data.

3 This ensures compliance with the legal requirements listed under section 1 of this policy.

Further information may be obtained from NHS Scotland's IT Security Manual, BS ISO/IEC 17799:2005, ITIL's Best Practice for Security Management and the Information Security Forum's - Standard of Good Practice for Information Security. These documents can be accessed through the IT Security Manager.