## CONFIDENTIALITY & DATA PROTECTION POLICY

<table>
<thead>
<tr>
<th>Lead Manager</th>
<th>Information Governance Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Director</td>
<td>Director of Health Information &amp; Technology</td>
</tr>
<tr>
<td>Approved by</td>
<td>Information Governance Steering Group</td>
</tr>
<tr>
<td>Date approved</td>
<td>July 2014</td>
</tr>
<tr>
<td>Date for Review</td>
<td>July 2017</td>
</tr>
<tr>
<td>Version</td>
<td>2.0</td>
</tr>
</tbody>
</table>
1.0 Introduction
Confidentiality is a fundamental principle in the delivery of health services. Much of the confidential information held relates to patients and employees of the service and this should be treated with respect to ensure its integrity, protection from inappropriate disclosure and it is readily available to authorised staff.

NHS Greater Glasgow & Clyde will take all reasonable measures to comply with its legal responsibilities and to preserve and maintain the confidentiality of the information it holds.

2.0 Scope
This policy applies to all staff employed by NHS Greater Glasgow & Clyde. It is also relevant to contractors, partnership organisations and visitors not employed by NHS Greater Glasgow & Clyde but engaged to work with, or who have access to health board information.

3.0 Policy Objectives
This policy aims to detail how NHS Greater Glasgow & Clyde meet its legal obligations and NHS requirements relating to confidentiality and information security standards. The requirements are primarily based upon the key piece of legislation, the Data Protection Act, 1998, however other relevant legislation and guidance may be referenced.

NHS Greater Glasgow & Clyde fully endorse the eight principles set out in the Data Protection Act and all staff who process personal information must ensure these principles are followed. In summary these state that personal data shall be: -

- Processed fairly and lawfully
- Processed for limited purposes and in an appropriate way
- Relevant and sufficient for the purpose
- Accurate and up to date
- Kept only for as longer as necessary
- Processed in line with individuals’ rights
- Secure
- Only transferred to countries that have suitable data protection controls

Furthermore, the Board is committed to adhering to the Caldicott principles for handling patient-identifiable data, namely: -

- Justify the purpose
- Only use when necessary
- Use the minimum required
- Access on a strict need to know basis
- Be aware of your responsibilities.
- Understand and comply with the law
- The duty to share information can be important as the duty to protect patient confidentiality

4.0 Roles and Responsibilities
4.1 Role of Chief Executive
The Chief Executive has overall responsibility for Data Protection. The Director of Health, Information and Technology has delegated functional responsibility for Data Protection.
4.2 Role of Caldicott Guardian
The Caldicott Guardian is responsible and accountable for the Board’s compliance with the Caldicott principles. This position is held by the Director of Health, Information and Technology and supported by the Boards Medical Director and Director of Public Health.

4.3 Role of Information Governance Manager
The Information Governance Manager is responsible for advising staff on relevant legislation, policies and guidance procedures for data protection and information security issues across NHS Greater Glasgow & Clyde, reporting to the Caldicott Guardian and the Information Governance Steering Group, on confidentiality issues.

4.4 Role of Directors and Heads of Departments
Senior managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

4.5 Role of Staff
Confidentiality is an obligation for all staff. Staff should note that they are bound by the NHSScotland Code of Practice: Protecting Patient Confidentiality. Staff have a confidentiality clause in their contract and are required to participate in induction and training to ensure they are kept updated on data protection and confidentiality issues.

5.0 Responsibilities
All employees working in NHS Greater Glasgow & Clyde are bound by a legal duty of confidence to protect and keep up to date personal information they may come into contact with during the course of their work. This is both a legal and contractual responsibility and also a requirement under the common law duty of confidence.

In order to ensure both new and current staff continue to receive appropriate training in data protection and confidentiality, NHS GGC will ensure there is a comprehensive training and awareness programme in place.

Person identifiable data is anything which contains the means to identify an individual, such as name, address or CHI number.

Confidential information within the NHS is commonly thought of as health data and can include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records and occupational health records.

Information can relate to patients and staff, including temporary staff, however stored. Information may be held on many formats including paper, CD/DVD, USB sticks, computer file or printout and mobile devices.

5.1 Principles
With respect to person identifiable or confidential data, all staff must ensure that:

- It is effectively protected against improper disclosure when it is received, stored, transmitted or disposed of
- Access is on a need-to-know basis
• Accurate and up to date information is maintained on staff and patients’ records
• Disclosure is limited to that purpose for which it is required
• Any disclosure can be justified
• Concerns are reported promptly to Line Management or the Information Governance Department
• Unwanted or confidential data is disposed of correctly

5.2 Disclosures
To enable the sharing of personal and other important information between agencies, the Board has Information Sharing Protocols in place with Local Authorities and other agencies which provide staff with detailed and specific guidance on the sharing of information between relevant parties.

To ensure information is shared appropriately with other parties, where an Information Sharing Protocol is not in place, care must be taken to ensure there is a legal basis for access to the information before releasing it.

5.2.1 Consider how much confidential information is required before disclosure and only disclose the minimum amount required.

5.2.2 Information can be disclosed:–
- When effectively anonymised
- When required by law or under a court order
- With the consent of the individual
- When in the public interest, such as concerns about a child or vulnerable adult
- Prevention and detection of serious crime

This list is not exhaustive and further advice can be sought from the Information Governance Department.

5.2.3 Ensure the method of transferring the information is secure and seek advice from the IT Security Manager if required. Some data transfers may require a Data Sharing Agreement to be in place and advice can be sought from the Information Governance Department.

5.2.4 Ensure appropriate standards and safeguards are in place in respect of telephone enquiries, emails, faxes and postal mail.

5.3 Working Away from Base
Staff may be required to work from another location or from home and as such carry with them confidential information. Staff should be aware that:–

• The taking home / removing paper documents containing person identifiable data should be discouraged as far as is practical
• Compliance with policies and procedures is still required
• Confidential data should stay with staff member when being transported
• Confidential data should be stored securely when at another location or at home when not being used
• Personal identifiable or confidential data should not be forwarded to a private email account
• Personal identifiable or confidential data should not be stored on a privately owned computer or device
5.4 **Carelessness**
Staff have a legal duty of confidence to keep person identifiable or confidential data private and not to divulge information accidentally and are reminded that they may be held personally liable for a breach of confidence.

5.5 **Abuse of Privilege**
Staff must not knowingly browse, search for or look at any information relating to themselves, their own family, friends, colleagues or others without a legitimate purpose. This will be viewed as a breach of confidentiality and of the Data Protection Act and will be dealt with in line with the Board’s Disciplinary Policy and Procedure.

6.0 **Associated Legislation / Policies / Standards**
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Copyright, Design and Patients Act 1988
- Data Protection Act 1998
- Freedom of Information (Scotland) Act 2002
- Human Rights Act 2000
- NHSIS IT Security Manual
- NHSScotland Caldicott Guardian’s Principles into Practice 2010
- NHSScotland Code of Practice: Protecting Patient Confidentiality
- Privacy and Electronic Communication Regulations 2003
- Public Records Scotland Act 2011
- Scottish Government Records Management: NHS Code of Practice (Scotland)
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

7.0 **Policy Review**
This policy will be reviewed on a bi-annual basis, unless the introduction of any new or amended relevant legislation warrants an earlier review.

8.0 **Communication and Implementation**
This Policy will be communicated through the Information Governance Framework.

9.0 **Further Advice**
For further advice on this Policy please contact the Information Governance Manager.
Tel: 0141 211 (5) 1790 Email: Isobel.brown@ggc.scot.nhs.uk