### Document Control Sheet

**Key Information:**

<table>
<thead>
<tr>
<th>Title:</th>
<th>Data Protection, Confidentiality and Privacy Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Status:</td>
<td>Approved</td>
</tr>
<tr>
<td>Document Type:</td>
<td>Policy</td>
</tr>
<tr>
<td>Version Number:</td>
<td>2.1</td>
</tr>
<tr>
<td>Author:</td>
<td>Jillian Neilson, Head of Information Governance</td>
</tr>
<tr>
<td>Owner:</td>
<td>Information Governance</td>
</tr>
<tr>
<td>Approved By:</td>
<td>Information Governance Operational Delivery Group</td>
</tr>
<tr>
<td>Date Effective From:</td>
<td>2015.10.05</td>
</tr>
<tr>
<td>Review Frequency:</td>
<td>2 years</td>
</tr>
<tr>
<td>Next Review Date:</td>
<td>2017.10.05</td>
</tr>
<tr>
<td>Contact:</td>
<td>Jillian Neilson, Head of Information Governance</td>
</tr>
</tbody>
</table>

**Revision History:**

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Summary of Changes</th>
<th>Responsible Officer</th>
</tr>
</thead>
</table>

**Approvals:** this document was formally approved by:

<table>
<thead>
<tr>
<th>Name/Title/Group</th>
<th>Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Governance Operational Delivery Group</td>
<td>2015.10.05</td>
<td>02.1</td>
</tr>
</tbody>
</table>

**Dissemination Arrangements:**

<table>
<thead>
<tr>
<th>Intended Audience</th>
<th>Method</th>
<th>Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>All NHS Ayrshire &amp; Arran staff</td>
<td>AthenA</td>
<td>2015.10.05</td>
<td>02.1</td>
</tr>
</tbody>
</table>

**Linked Documentation:**

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Document File Path</th>
</tr>
</thead>
</table>

**NB. This document is uncontrolled when printed.** The contents of this document are subject to change, any paper copy is only valid on the day of printing. To ensure you have the most up to date version of this document please use the link to access the document directly from AthenA.
Table of Contents

Table of Contents ............................................................................................ 3
1  Introduction.................................................................................................. 4
2  Purpose ...................................................................................................... 4
3  Scope of the Policy .................................................................................... 5
4  Definition of Terms .................................................................................. 5
5  Legal Context ............................................................................................ 6
6  Responsibilities ......................................................................................... 7
7  Implementation .......................................................................................... 8
8. Access to Information ............................................................................... 9
9. Supporting Operating Procedures ............................................................ 9
10. Related Legislation and Policy ............................................................... 9
Appendix 1 – The Principles ............................................................................ 11
1 Introduction

1.1 NHS Ayrshire and Arran processes large volumes of sensitive and personal identifiable information that is confidential information relating to patients, employees, suppliers and others with whom it communicates in the provision of services. In addition, it may be a legal requirement to collect and use certain types of information in compliance with this legislation. This personal information no matter how it is collected, recorded or used must be treated with respect to ensure integrity, and to make sure that it is not available to persons unauthorised to see it.

1.2 NHS Ayrshire and Arran is an open organisation and encourages dissemination of the information it holds. It is also a responsible organisation, and respects the private life of all living individuals. It therefore seeks to ensure that personal and sensitive information is not divulged without just cause and that it complies with the requirements of all current data protection in force at any given time.

1.3 This policy details how NHS Ayrshire and Arran will meet its legal obligations and NHS requirements concerning data protection, confidentiality and privacy.

2 Purpose

2.1 The aims and objectives of this policy are to ensure that:

- The principles that govern all uses of personal identifiable information are clearly understood by all.


- Staff members clearly understand through this policy our commitment towards effective data protection, confidentiality and privacy compliance.

- Staff members who manage and/or process personal identifiable information understand their responsibilities in relation to data protection, confidentiality and privacy; that they are contractually responsible for following good data protection practice and are appropriately trained and effectively supervised.

- That the rights of any individual are observed in line with the Data Protection Act 1998 principles (See Appendix 1) and that they know who to approach regarding these rights and that they are promptly and courteously dealt with.
3 Scope of the Policy

3.1 This policy covers all employees, volunteers and any contractors supplying services or carrying out work on behalf of NHS Ayrshire and Arran.

4 Definition of Terms

4.1 Personal Data – as defined by the Data Protection Act 1998, is data which relates to an individual who can be identified from those data or from those data and other information which is in the possession of the data controller and includes any expression or opinion about the individual and any indication of the intentions of the data controller or any other person in respect of that individual. Some common personal data items are:

- Name
- Address
- Date of birth
- CHI number.

Sensitive Personal Data

The 1998 Act defines ‘sensitive personal data’ as information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions. Under the Act the processing of this “sensitive personal data” is subject to more stringent conditions.

4.2 Processing – in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.

4.3 Data Controller – Person(s) that determine the purposes for which, and manner in which any personal data may be processed. “NHS Ayrshire & Arran” as the organisation is the Data Controller.

4.4 Data Processor - A Data Processor in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

4.5 Caldicott - The Caldicott report, commissioned by the Chief Medical Officer for Health in England & Wales, raised concerns regarding the way information flowed, not only within NHS organisations, but also between non-NHS organisations. The Caldicott report did not extend to Scotland but the Scottish Executive adopted its 16 recommendations and 7 general principles for the safe handling of patient identifiable information. They work hand in hand with the Principles of the Data
Protection Act 1998, and both cover information held on paper as well as electronically. All staff must adhere to these principles. (See Appendix 1)

5 Legal Context

5.1 Data Protection Act 1998 – The Data Protection Act 1998 establishes a framework of rights and duties which are designed to safeguard personal information. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details. The Act only applies to “personal data” (see 4.1) held about identifiable living individuals. In order to comply with the Act, NHS Ayrshire and Arran has a duty to keep all personal information held on patients and staff confidential and secure. Employees must ensure they do not pass on information to anyone else unless authorised to do so and must also ensure that all personal details are processed in accordance with the rights of the data subjects as defined under the Act.

The organisation and the staff employed within NHS Ayrshire and Arran must abide and adhere to the rules of “good information handling” known as the Data Protection Principles: (See Appendix 1)

5.2 Human Rights Act 1998 - Article 8.1 of the European Convention on Human Rights, as given effect to by the Human Rights Act 1998, provides that “everyone has the right to respect for his private and family life, his home and his correspondence.”

5.3 Common Law duty of Confidentiality - Common law is not based on statute and Acts of Parliament, it is based on the decisions made by the courts on specific cases, and is developed over time. This law underpins the duty of confidentiality that states that -

‘If information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider’s consent.’

Information is confidential when it is not in the public domain, not common knowledge and is worthy of protection due to the damage, harm or distress that disclosure might cause.

This duty extends to all staff who work for NHS Ayrshire and Arran.
6 Responsibilities

6.1 Chief Executive
The Chief Executive has overall responsibility for the Data Protection Confidentiality and Privacy Policy within NHS Ayrshire and Arran.

6.2 Caldicott Guardian
The Caldicott Guardian is responsible for ensuring that NHS Ayrshire and Arran satisfies the highest practical standards for handling patient information standards in compliance with the Caldicott Principles.

6.3 Head of Information Governance
The implementation of, and compliance with, this policy is delegated to the Head of Information Governance who will act as data protection lead. The Head of Information Governance has responsibility for chairing the Information Governance Operational Delivery Group which has responsibility for bringing data protection issues to the NHS Ayrshire and Arran Board via the Information Governance Committee. The Information Governance Team will provide training and training materials for staff in relation to data protection, confidentiality and privacy.

6.4 Managers
The day to day responsibilities for enforcing this policy will be devolved to managers. Managers will ensure that their teams undertake training to ensure staff are aware of their responsibilities and the most effective way of ensuring adequate information security and confidentiality.

6.5 Staff
Staff members must comply with the requirements of their contract in relation to ‘duty of confidentiality’ and to adhere to this policy and the related documents and procedures listed in Section 10. Staff will also be expected to participate in any training required in order to achieve a standard of knowledge and understanding in these issues relative to the duties of their post.
7 Implementation

7.1 All staff contracts will include an employee commitment to confidentiality and to abide by the principles laid down in the Data Protection Act 1998. To ensure that knowledge of these guidelines and procedures is kept up to date, staff will be required to sign a confidentiality statement. It is the responsibility of all those referred to in Section 3 of this policy to ensure compliance with all legislation, related policy, procedures, protocols and supporting guidance contained and referenced in this policy document.

7.2 Any staff transferring between NHS organisations, any appointments of temporary staff, agency staff, students or trainees, must be made aware of this policy and other related documents by the appropriate line manager/supervisor.

7.3 The Head of Information Governance will ensure that a full, correct and up-to-date notification is lodged for NHS Ayrshire and Arran with the Information Commissioner.

7.4 All contracts with external suppliers must comply with CEL 25 (Safeguarding the Confidentiality of Personal Data Processed by Third Party Contractors).

7.5 NHS Ayrshire and Arran are mandated by the Scottish Government (MEL (1999) 19) to ensure that there is always a nominated ‘Caldicott Guardian who will have ultimate responsibility for maintaining the confidentiality of patient identifiable data held within the organisation.

7.6 NHS Ayrshire and Arran are also mandated by the Scottish Government (HDL (2006) 41) to appoint a person with specific responsibility for advising on and monitoring data protection. Within NHS Ayrshire & Arran this is the Head of Information Governance.

7.7 This policy will be reviewed biannually to ensure that it continues to be effective and comply with existing legal requirements

7.8 A regular review and audit will be made of the way in which personal identifiable information is managed in relation to data protection compliance.

7.9 Operational procedures and guidelines will be put in place to underpin this policy.

7.10 Where deemed appropriate by management, breaches of the legislation covered in this policy and any associated policy may result in action being taken through current disciplinary procedures as outlined in the NHS Ayrshire and Arran ‘Management of Employee Conduct Policy’.
8. **Access to Information**

8.1 Under the Data Protection Act 1998, individuals have a right to see or be provided with a copy of personal information the organisation holds about them, this is known as a ‘Subject Access Request’. Information and guidance for handling Subject Access Requests are available from the AthenA intranet using the following link:

http://athena/kmeh/kmeh/igs/Pages/SARs.aspx

9. **Supporting Operating Procedures**

9.1 This Policy will be supported by the following operating procedures:

- Subject Access Request Policy and Standard Operating Procedures
- Non Disclosure Agreement Procedures
- Freedom of Information Access Request Procedures
- Information Security Breach Procedures
- Information Sharing Protocols

10. **Related Legislation and Policy**

10.1 This policy should be read in conjunction with the following:

**Local**

- NHS Ayrshire & Arran - Secure Storage, Communication & Transportation of Personal Information Policy.
- NHS Ayrshire & Arran – Management of Employee Conduct Policy
- NHS Ayrshire & Arran - Closed Circuit TV Policy
- NHS Ayrshire & Arran - Freedom of Information Policy
- NHS Ayrshire and Arran - E-Mail Management Policy
- NHS Ayrshire and Arran - Password Policy
- NHS Ayrshire and Arran - Appropriate Use of IT Facilities Policy
- NHS Ayrshire and Arran - Document Scanning Guidelines
- NHS Ayrshire and Arran - Social Media Policy
National

- Data Protection Act 1998
- Freedom of Information (Scotland) Act 2002
- Adults with Incapacity (Scotland) Act 2000.
- Public Records (Scotland) Act 1937.
- Disposal of Records (Scotland) Regulations 1992
- Protecting Patient Confidentiality: NHSScotland Code of Practice
- The Regulation of Investigatory Powers (Scotland) Act 2000
- Computer Misuse Act 1990
- Access to Medical Reports Act 1988
- Access to Health Records Act 1990
- Crime and Disorder Act 1998
- Criminal Justice and Immigration Act 2008
- Information Commissioner’s Office - Employment Practices Code
- CEL 13 2008 Information sharing between NHS Scotland and the Police
- Information Security : NHS Code of Practice
- CEL 25 (2011) NHS Scotland: Safeguarding the Confidentiality of Personal Data processed by Third Party Contractors.
- Scottish Government Records Management : NHS Code of Practice (Scotland) Version 2.1
Appendix 1 – The Principles

Data Protection Act 1998 – The Principles

1. Personal data must be processed fairly and lawfully.
2. Personal data shall be obtained for only one or more lawful purpose and must not be further processed for incompatible purposes.
3. Personal data shall be adequate, relevant, and not excessive.
4. Personal data shall be accurate, and where necessary, kept up to date.
5. Personal data shall not be kept for longer than necessary.
6. Personal data shall be processed in accordance with the rights of data subjects under the Act, they can:
   ▪ See and get a copy of information held about them.
   ▪ Prevent processing in particular circumstances
   ▪ Seek compensation where processing has caused damages or distress
   ▪ Have inaccurate information rectified, blocked or destroyed

7. Appropriate technical and organisational measures shall be taken to prevent unauthorised or unlawful processing of data and against accidental loss or destruction of, or damage to data.
8. Personal data shall not be transferred to a country outside the European Economic Area, unless that country ensures an adequate level of protection for the rights and freedom of individuals in relation to processing the data.

Caldicott – The Principles

1. Justify the purpose(s) for using confidential information
2. Only use it when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need-to-know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law
7. Duty to share is as important as duty of confidentiality