Data Protection, Confidentiality and Privacy Policy
### Document Control Sheet

<table>
<thead>
<tr>
<th>Title:</th>
<th>Data Protection, Confidentiality and Privacy Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Status:</td>
<td>Final</td>
</tr>
<tr>
<td>Document Type:</td>
<td>Policy</td>
</tr>
<tr>
<td>Version Number:</td>
<td>v03.2</td>
</tr>
<tr>
<td>Author:</td>
<td>Head of Information Governance &amp; Data Protection Officer</td>
</tr>
<tr>
<td>Owner:</td>
<td>Head of Information Governance &amp; Data Protection Officer</td>
</tr>
<tr>
<td>Approved By:</td>
<td>Information Governance Operational Delivery Group</td>
</tr>
<tr>
<td>Date Approved:</td>
<td>05/09/2019</td>
</tr>
<tr>
<td>Status:</td>
<td>Final</td>
</tr>
<tr>
<td>Page:</td>
<td>2 of 11</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>
<tbody>
<tr>
<td>02.1</td>
<td>2015.10.05</td>
<td>Change to template, removal of Appendix 2.</td>
<td>Jillian Neilson</td>
</tr>
<tr>
<td>03.0</td>
<td>2018.05.02</td>
<td>Change to template. Updated to reflect changes to Data Protection legislation</td>
<td>Jillian Neilson, Head of IG &amp; DPO</td>
</tr>
<tr>
<td>03.2</td>
<td>2019.08.13</td>
<td>Minor changes to ensure compliance with Data Protection legislation</td>
<td>Marie Lynch, IG Analyst</td>
</tr>
</tbody>
</table>

#### Approvals:

This document was formally approved by:

<table>
<thead>
<tr>
<th>Name &amp; 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>
<tr>
<td>Information Governance Operational Delivery Group</td>
<td>2018.05.02</td>
<td>03.0</td>
</tr>
<tr>
<td>Information Governance Operational Delivery Group</td>
<td>2019-09-05</td>
<td>03.2</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 A&amp;A staff</td>
<td>AthenA</td>
<td>2015.10.05</td>
<td>02.1</td>
</tr>
<tr>
<td>All NHS A&amp;A staff</td>
<td>AthenA</td>
<td>2018.05.02</td>
<td>03.0</td>
</tr>
<tr>
<td>All NHS A&amp;A staff</td>
<td>AthenA</td>
<td>2019-09-05</td>
<td>03.2</td>
</tr>
<tr>
<td>Public dissemination</td>
<td>NHS A&amp;A Public Website</td>
<td></td>
<td>03.2</td>
</tr>
</tbody>
</table>

#### Linked Documentation:

<table>
<thead>
<tr>
<th>Document Title:</th>
<th>Document File Path:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</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 or contact the Author.
Contents

1.0 Introduction............................................................................................................................................... 4
2.0 Purpose .................................................................................................................................................... 4
3.0 Scope ....................................................................................................................................................... 4
4.0 Definition of Terms .................................................................................................................................. 4
5.0 Roles & Responsibilities ............................................................................................................................ 5
6.0 Legal Context, Implementation & Access .................................................................................................. 6
7.0 Related Documents .................................................................................................................................... 9
8.0 Appendix 1 The General Data Protection Principles ................................................................................. 10
1.0 Introduction

1.1 NHS Ayrshire & Arran (NHS A&A) process a large volume of personal identifiable and special category personal data that relates 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 access it.

1.2 NHS A&A 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 individuals. NHS A&A seeks to ensure that personal and special category personal data is not divulged without just cause and complies with the requirements of all current data protection legislation in force at any given time.

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

2.0 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 Data Protection Legislation and that they know who to approach regarding these rights and that they are promptly and courteously dealt with.

3.0 Scope

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

4.0 Definition of Terms

4.1 Personal Data – as defined by Data Protection Legislation, 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 identifiers are:

- Name
- Address
- Date of birth
- CHI number

4.2 **Special Categories of Personal Data**
Data Protection Legislation defines “special categories of personal data” as information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions. Under Data Protection Legislation the processing of “special categories of personal data” is subject to more stringent conditions.

4.3 **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.

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

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

4.6 **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.

5.0 **Roles & Responsibilities**

5.1 **Chief Executive**
The Chief Executive has overall responsibility for the Data Protection Confidentiality and Privacy Policy within NHS A&A.

5.2 **Caldicott Guardian**
The Caldicott Guardian is responsible for ensuring that NHS A&A satisfies the highest practical standards for handling patient information standards in compliance with the Caldicott Principles.

5.3 **Senior Information Risk Owner (SIRO)**
By delegation from the Chief Executive takes overall ownership for organisational information risk.
5.4 **Head of Information Governance & Data Protection Officer**
The implementation of this policy is delegated to the Head of Information Governance, who has also been designated the Data Protection Officer (DPO). The Head of Information Governance & DPO has responsibility for chairing the Information Governance Operational Delivery Group which has responsibility for bringing data protection issues to the NHS A&A 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.

**Data Protection Officer**
Article 37 of General Data Protection Regulation requires public authorities to designate a qualified expert Data Protection Officer. A key role of the DPO is to provide advice and inform staff, partners and subcontractors and monitor the processing of information in compliance with the regulations and on risks associated with the processing of information.

5.5 **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.

5.6 **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 7. 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.

6.0 **Legal Context, Implementation & Access**

**Legal Context**

6.1 **General Data Protection Regulation (GDPR)**
The EU General Data Protection Regulation (GDPR) became directly applicable as law in the UK on 25th May 2018. The GDPR requires that organisations (data controllers) that process personal data demonstrate compliance with its provisions (the Six GDPR Principles listed in Appendix 1). Part of this involves establishing and publishing a basis for lawful processing, and where relevant, a condition for processing special categories data.

6.2 **Data Protection Act 2018**
The Data Protection Act 2018 (DPA18) addresses areas in which flexibility and derogations are permitted from within the GDPR.

6.3 **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.”

6.4 **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 A&A.

6.5 **Public Records Scotland Act 2011**
The Public Records (Scotland) Act 2011 requires all Scottish Public Authorities to produce and submit a Records Management Plan (RMP) to the Keeper of the Records of Scotland. This plan must detail their current position and how they will work towards fulfilling all of the requirements of the Act by setting out proper arrangements for the management of it's public records. This applies to all health and corporate records irrespective of the technology used to create and store them or the type of information they contain. NHS A&A's Records Management Plan was agreed by the Keeper of the Records of Scotland on 3rd October 2016.

**Implementation**

6.6 All staff contracts will include an employee commitment to confidentiality and to abide by the principles laid down in Data Protection Legislation. 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 5 of this policy to ensure compliance with all legislation, related policy, procedures, protocols and supporting guidance contained and referenced in this policy document.

6.7 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.

6.8 The Head of Information Governance & DPO will ensure that a full, correct and up-to-date registration is lodged for NHS A&A with the Information Commissioner’s Office.

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

6.10 NHS A&A 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.

6.11 NHS A&A are also required to designate a qualified expert Data Protection Officer as stated within Article 37 of GDPR. Within NHS A&A this is the Head of Information Governance.

6.12 NHS A&A will maintain records of their processing activities within an Information Asset Register.

6.13 NHS A&A will adopt data protection by design and default methodologies when developing or changing how personal information is processed by the organisation. Data Protection Impact Assessments will be completed where necessary and appropriate.

6.14 NHS A&A will provide a Data Protection Notice providing the fair processing information to data subjects in compliance with the GDPR.

6.15 NHS A&A will retain personal and special category personal data only for as long as needed. Information is retained in line with the Scottish Government Records Management: NHS Code of Practice (Scotland) Version 2.1 January 2012. The NHS Code of Practice sets out minimum retention periods for information, including personal information, held in different types of records including personal health records and administrative records. As directed by the Scottish Government in the Records Management Code of Practice, we maintain a retention schedule detailing the minimum retention period for the information and procedures for the safe disposal of personal information.

Link to Operational Procedure for the Destruction of Personal Health Records
Link to Corporate Records Retention and Disposal Policy

Link to Scottish Government Records Management: NHS Code Of Practice http://www.gov.scot/Publications/2012/01/10143104/0

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

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

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

6.19 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 A&A ‘Management of Employee Conduct Policy’.
Access to Information

6.20 Under the Data Protection Legislation, 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 is detailed within NHS A&A Access to Personal Information held about you policy document.

7.0 Related Documents

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

NHS A&A Policy
- NHS A&A Secure Storage, Communication & Transportation of Personal Information Policy
- NHS A&A Corporate Records Management Policy
- NHS A&A Management of Employee Conduct Policy
- NHS A&A Closed Circuit TV Policy
- NHS A&A Freedom of Information Policy
- NHS A&A E-Mail Policy & Best Practice Guidance
- NHS A&A Password Policy
- NHS A&A Information Security Policy
- NHS A&A Appropriate Use of IT Facilities Policy
- NHS A&A Social Media Policy

Legislation
- Data Protection Act 2018
- General Data Protection Regulation
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Freedom of Information (Scotland) Act 2002
- Public Records (Scotland) Act 2011
- Public Bodies (Joint Working) (Scotland) Act 2014 Provision 49 Information Sharing
- 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
- Adults with Incapacity (Scotland) Act 2000.
- Disposal of Records (Scotland) Regulations 1992
Directives

- CEL 25 (2011) - Safeguarding The Confidentiality Of Personal Data Processed By Third Party Contractors
- CEL 26 (2011) NHS Scotland Information Assurance Strategy
- CEL (2008) 13 Information sharing between NHS Scotland and the police
- CEL (2007) 11 Provision of Medical Records by NHS to Courts
- MEL (1997) 45 Guidance on the Use of Facsimilie Transmissions

Scottish Government Guidelines

- Information Governance, Roles and Responsibilities within Health & Social Care: Code of Practice (Scotland) 2017
- Using Email in NHSScotland: A Good Practice Guide
- Short Messaging Service Good Practice Guide
- Reporting Significant eHealth Information Security Incidents in NHSScotland

Information Commissioner's Office Codes of Practice available at: www.ico.org.uk

Appendix 1 The General Data Protection Principles
Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that:
the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

**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