Data Protection Policy

Date Published: May 2018
Version: V 2.1
Owner: Associate Director of Corporate Affairs and Compliance/ Acting Senior Information Risk Owner (SIRO)
Author: Patricia Ruddy, NSS Head of Data Protection / Data Protection Officer
## DOCUMENT CONTROL SHEET

### Key Information:

<table>
<thead>
<tr>
<th>Title:</th>
<th>Data Protection Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Published/Issued:</td>
<td>May 2018</td>
</tr>
<tr>
<td>Date Effective From:</td>
<td>May 2018</td>
</tr>
<tr>
<td>Version/Issue Number:</td>
<td>2.1</td>
</tr>
<tr>
<td>Document Type:</td>
<td>Policy</td>
</tr>
<tr>
<td>Document Status:</td>
<td>Final</td>
</tr>
<tr>
<td>Author:</td>
<td>Patricia Ruddy, NSS Head of Data Protection/ Data Protection Officer</td>
</tr>
<tr>
<td>Owner:</td>
<td>Associate Director of Corporate Affairs and Compliance/ Acting Senior Information Risk Owner (SIRO)</td>
</tr>
<tr>
<td>Approver:</td>
<td></td>
</tr>
<tr>
<td>Approved by and Date:</td>
<td>May 2018</td>
</tr>
<tr>
<td>Contact:</td>
<td></td>
</tr>
<tr>
<td>File Location:</td>
<td></td>
</tr>
</tbody>
</table>

### Revision History

<table>
<thead>
<tr>
<th>Version:</th>
<th>Date:</th>
<th>Summary of Changes:</th>
<th>Name:</th>
<th>Changes Marked:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>3.06.13</td>
<td>Review and revision of policy</td>
<td>NSS Privacy Advisor</td>
<td></td>
</tr>
<tr>
<td>1.1 draft</td>
<td>28.10.15</td>
<td>Review and revision of policy – SBU consultation stage</td>
<td>NSS Privacy Advisor</td>
<td>Yes</td>
</tr>
<tr>
<td>1.2 draft</td>
<td>14.12.15</td>
<td>Review and revision of policy and transfer to new policy template – IGG review</td>
<td>NSS Privacy Advisor</td>
<td>No</td>
</tr>
<tr>
<td>1.3</td>
<td>January 2016</td>
<td>Review and revision of policy and transfer to new policy template – IGG revisions included, for consideration by Corporate Policy Group</td>
<td>NSS Privacy Advisor</td>
<td>No</td>
</tr>
<tr>
<td>2.0 draft</td>
<td>2018</td>
<td>Review and revision of policy – preparation for GDPR</td>
<td>NSS Privacy Advisor</td>
<td>No</td>
</tr>
<tr>
<td>2.1 draft</td>
<td>2018</td>
<td>Pre-consultation comments made by Data Protection Leads and Caldicott Guardians</td>
<td>NSS Privacy Advisor</td>
<td>No</td>
</tr>
<tr>
<td>2.1 final</td>
<td>May 2018</td>
<td>Finalised version following formal consultation period</td>
<td>NSS Head of Data Protecti</td>
<td>No</td>
</tr>
</tbody>
</table>
**Distribution:** This document has been distributed to:-

<table>
<thead>
<tr>
<th>Name</th>
<th>Title/SBU</th>
<th>Date of Issue</th>
<th>Version:</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSS DP Leads and Caldicott Guardians</td>
<td></td>
<td>January 2018</td>
<td>2.0 draft</td>
</tr>
<tr>
<td>NSS Corporate Compliance Group</td>
<td></td>
<td>February – March 2018</td>
<td>2.1 draft</td>
</tr>
<tr>
<td>NSS Information Governance Committee</td>
<td></td>
<td>April 2018</td>
<td>2.1 final</td>
</tr>
<tr>
<td>NSS Partnership Forum</td>
<td></td>
<td>April 2018</td>
<td>2.1 final</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>
</tbody>
</table>
1. **SUMMARY**

NHS National Services Scotland (NSS) is required to comply with data protection law. Data protection law balances the need of organisations to collect and use personal data for clearly defined purposes with the right of individuals to privacy.

From 25 May 2018, the EU General Data Protection Regulation (GDPR) introduces new data protection law which extends the rights of, and protections for, all living individuals’ personal data. The UK is also enacting a new Data Protection Act in 2018, which implements the GDPR and other related European privacy law.

Until then, the Data Protection Act 1998 (DPA 1998) applies. The DPA came into force on 1 March 2000 and was set up to establish a framework of rights and duties in order to protect all living individuals’ personal data.

This policy sets out the NSS approach to the handling of personal data in compliance with data protection law. It applies to all services provided and supported by NSS and all staff who work for or under contract to NSS, including contractors, students, agency, bank staff and volunteers.

2. **AIM OF THE POLICY**

NSS uses patient and donor data for a variety of administrative, research and medical purposes. In addition, NSS needs to collect, process and keep a variety of sensitive and personal data about people in order to carry out its functions as a public authority and perform business operations in support of these. This includes data on employees, suppliers, contractors, donors, patients, clients/ customers and others with whom it communicates. The aim of the policy is to help ensure that all such personal data is dealt with lawfully, properly and securely no matter how it is collected, recorded and used – whether on paper, on electronic devices such as a computer or laptop, or recorded in other ways.

Should members of staff have any difficulties with understanding any aspect of this policy, or its application, they should discuss this with their Line Manager and if necessary seek further advice from Strategic Business Unit (SBU)/ Directorate data protection/ information governance leads or organisational information governance leads e.g. NSS Data Protection Officer.
3. SCOPE OF THE POLICY

The policy covers:

- All services provided and supported by NSS
- All staff who work for or under contract to NSS, including contractors, students, agency, bank staff and volunteers

All staff must meet the standards of practice outlined in this document as well as those included within their terms of employment. Those who are registered healthcare professionals must also keep to their own regulatory organisation's standards of conduct and practice.

4. DEFINITIONS OF PERSONAL DATA

Data protection law applies to 'personal data'. It applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include time-ordered sets of manual records containing personal data.

From 25 May 2018, ‘personal data’ means information relating to an identifiable, living person who can be directly or indirectly identified, in particular by reference to an identifier. A wide range of personal identifiers meet the definition of personal data, including name, identification number, location data or online identifier.

Stricter conditions apply to the use of 'special categories' of personal data. These are defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the use of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health and or data concerning a natural person's sex life or sexual orientation. Similar, stricter conditions also apply to personal data relating to criminal convictions and offences.

The relevant definitions set out in the DPA 1998, which applies until 25 May 2018, are included in Appendix 1.
Directly and indirectly identifiable

Some items of information about people, for example ‘name’, identify them directly, and are therefore personal data and protected by data protection law. Other items of information, such as date of birth and full postcode, may lead to the indirect identification of a person, and must therefore be treated with care. Where statistics are derived from a small number of individuals, indirect identification of individuals may also become possible.

When questions arise on the risk of indirect identification, an assessment needs to be made on the information and the risk of disclosure of an individual’s identity. This includes a review, informed by senior staff, such as the Caldicott Guardian, within the Strategic Business Unit (SBU) or Directorate, and the application of statistical disclosure controls where appropriate. This enables a decision to be made on how the information is to be handled.

5. DATA PROTECTION PRINCIPLES

NSS must carry out its functions as a public authority, and its business operations in support of these, in compliance with the following principles. From 25 May 2018 these state that personal data must 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 shall not be considered to be incompatible with those 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 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 the implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(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.

Data protection law also requires that compliance with these principles can be demonstrated through evidence such as policies, procedures and relevant documentation of processing activities.

The principles set out in the DPA 1998, which applies until 25 May 2018, are included in Appendix 1.

6. POLICY STATEMENT AND COMMITMENT

In order to fulfil its obligations under data protection law NSS is committed to:

- Making people aware when collecting personal data about them, and outlining the ways in which that information will be used;

- Observing fully conditions regarding the fair collection and use of personal data; in particular ensuring that in its publication and release of information, adequate steps- including an assessment of risks, record-keeping of considerations and techniques such as redaction and anonymisation - are taken to minimise the risks to individuals’ privacy;

- Meeting its legal obligations to specify the purposes for which personal data are used;
• Collecting and processing appropriate personal data, only to the extent that it is needed to carry out our functions as a public authority, fulfil operational needs or to comply with any legal requirements;

• Retaining personal data only for as long as needed;

• Ensuring that people about whom it holds personal data can exercise their rights fully under data protection law;

• Taking appropriate technical and organisational measures to safeguard personal data;

• Ensuring that personal data are not transferred abroad without suitable safeguards.

This is achieved through:

• The use of privacy notices to inform people about the collection and use of their personal data, detailing all of the information to which they are entitled under data protection law.

• Until 25 May 2018, notification with the Information Commissioner of all processing of personal data within NSS. The notification number for NSS is Z5801192.

• The identification of a designated Data Protection Officer (DPO), responsible for advising on and monitoring data protection practice in the organisation. NSS is required to ensure that the DPO is resourced adequately, operates independently and reports to the highest management level of NSS i.e. board level.

• Training for all NSS staff in information handling, information security, information governance and compliance, to ensure that everyone understands their responsibility under data protection law.

• In accordance with NSS Records Management and Information Security policies, the appropriate retention, and thereafter disposal, of personal data that is out of
date and of no essential value to the legitimate operation of the organisation.

- The implementation of procedures to safeguard the rights conferred on people by data protection law.

- The maintenance of relevant documentation about the processing of personal data by NSS, including keeping an up to date Information Asset Register (IAR), appropriate data sharing agreements and contractual documentation.

- The appropriate integration of data protection into processing activities, including the conduct of data protection impact assessments (DPIAs) where appropriate, helping to ensure privacy by design.

- The notification of the Information Commissioner's Office, and in some cases the person/people affected, when certain types of personal data breach have occurred. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- The regular monitoring, review and audit of the way in which personal data are collected, stored and used by NSS.

7. SPECIFIC RESPONSIBILITIES

Chief Executive
The Chief Executive has overall accountability for NSS’s compliance with data protection law, the common law duty of confidentiality and associated regulations.

Directors
The Chief Executive delegates day-to-day responsibility for NSS’s operational compliance to his direct reports. They are responsible for the day-to-day management of the risks associated with the processing of personal data, and for ensuring the development of specific operational procedures required for the proper processing of personal data in their area. Directors must ensure there are clear procedures in their
area for enabling safe, appropriate access to personal data and that the Data Protection Leads in their SBU/ Directorate undertake the training required for their role.

**NSS Information Governance Committee**

The NSS Information Governance Committee, a Board sub-Committee, monitors the compliance of NSS with its data protection obligations, along with the other information governance regulatory and policy obligations that are monitored as part of its remit.

**NSS Senior Information Risk Owner (SIRO)**

The NSS SIRO ensures that NSS information assets and risks are managed such that data protection compliance obligations are considered appropriately.

**NSS Associate Director of Corporate Affairs and Compliance**

The NSS Associate Director of Corporate Affairs and Compliance ensures that all policies and procedures concerning compliance with information governance and data protection law are produced, approved, implemented and monitored.

**Information Asset Owners (IAOs)**

NSS Information Asset Owners, identified in our Information Asset Register (IAR), ensure that those information assets which comprise personal data for which they are responsible are managed in compliance with data protection law.

**NSS Head of Data Protection/ Data Protection Officer (DPO)**

The Data Protection Officer (DPO) has specific responsibility for:

- Informing and advising NSS and its staff about their obligations to comply with data protection law
- Monitoring compliance with data protection law
- Being the first point of contact for the Information Commissioner’s Office (ICO) and people whose personal data are processed by NSS.

**SBU and Directorate Data Protection Leads**

The SBU and Directorate Data Protection Leads support and inform the work of the NSS Head of Data Protection/ Data Protection Officer (DPO). They are responsible for the promotion of data protection good practice in their area and assisting with any investigations and reviews concerning NSS’s compliance with data protection law. They also help to ensure adequate training is provided to relevant personnel and a
general awareness is given to all NSS staff.

**Line Managers**
Managers at all levels are responsible for ensuring they understand this Policy and that the staff for whom they are responsible are aware of, understand and adhere to it. They are also responsible for ensuring staff are updated and supported in regard to understanding and implementing any changes in this policy.

**All NSS staff and individuals engaged to work on its behalf**
All staff who work for or under contract to NSS, including contractors, students, agency, bank staff and volunteers are responsible for ensuring that they are aware of and understand the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis, seeking support when necessary.

All staff have a duty to report any suspected or actual adverse events associated with the processing of personal data, as specified in the NSS Adverse Events Management Policy. Adverse events include, but are not limited to, the loss or non-delivery of a document containing personal data in the post, or via e-mail, and a mistaken disclosure of personal data to an individual or organisation not entitled to receive it.

Breaches of this policy, and therefore data protection law, may lead to disciplinary action, in line with the NSS Management of Employee Conduct Policy

8. **MONITORING OF THIS POLICY**

The NSS Associate Director of Corporate Affairs and Compliance will monitor this policy and any associated procedures. It is also assumed that both internal and external audit will review this and associated policies and procedures, when appropriate.

9. **POLICY REVIEW**

This policy will be reviewed **one year** from its effective date to ensure it supports adequately compliance with the new data protection law which comes into force on 25th May 2018, and thereafter every two years to ensure that arrangements remain appropriate to the operating requirements of National Services Scotland.
Date policy is effective:

Reviewed by:

Agreed by: [Signature]
Chair, Staff Governance Committee

Date: 11/8/15
APPENDIX 1: Data Protection Act 1998 (DPA 1998)

The Data Protection Act 1998 (DPA 1998) is superseded from 25 May 2018. Until that time the Data Protection Act 1998 (DPA) is the data protection law that applies to our use of personal data. Relevant details of the DPA 1998 are given below.

DPA 1998 Definitions of Personal Data

Under the DPA “personal data” are defined as “data which relate to a living individual who can be identified:

(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession, of the data controller”

This includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Stricter conditions apply to the processing of ‘sensitive personal data’. Under section 2 of the DPA, “sensitive personal data” are defined as personal data consisting of information as to –

(a) the racial or ethnic origin of the data subject;
(b) his political opinions;
(c) his religious beliefs or other beliefs of a similar nature;
(d) whether he is a member of a trade union;
(e) his physical or mental health or condition;
(f) his sexual life;
(g) the commission or alleged commission by him of any offence;
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

DPA 1998 Data Protection Principles

Schedule 1 of the DPA outlines eight principles which underpin the handling of personal data. In order to achieve compliance NSS must ensure that its use of personal data meets the standards set out in these principles which are:

Principle 1 Personal data shall be processed fairly and lawfully.

Principle 2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
**Principle 3** Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

**Principle 4** Personal data shall be accurate and, where necessary, kept up to date.

**Principle 5** Personal data shall not be kept for longer than is necessary for that purpose or those purposes.

**Principle 6** Personal data shall be processed in accordance with the rights of data subjects under the Act.

**Principle 7** Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

**Principle 8** Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
APPENDIX 2: USEFUL POLICIES, GUIDANCE AND WEB SITES

Information Governance Policy
Confidentiality Policy
NSS Adverse Events Management Policy
Information Security Policy
IT Acceptable Use Policy and Guidelines
Document Storage, Retention and Disposal Policy
NSS Data Protection Subject Access Request Form and Guidance to Staff
NSS Employee Data Handling within Human Resources
NSS Data Protection/ Privacy Impact Assessment Guidance
NSS Statistical Disclosure Control Protocol
NSS Data Processing Undertakings
NSS CCTV Policy
NSS Data Protection Information Notice
NSS Data Sharing Good Practice Guide

The following website may also be of interest:
Information Commissioner’s Office