NRS Data Protection Policy

May 2023

Document Control

Title	NRS – Data Protection Policy

Document Owner

Name	Role	Branch / Directorate
Laura Mitchell	Director of Information and Records Services	Information and Records Services

Document Reviewers

Role
Head of Information Governance

Status Control

Version	Date	Status	Prepared By	Role	Reason for Amendment
1.0	21/08/2018	Final	John Simmons	Head of Information Governance	To incorporate changes proposed by Data Protection Officer
2.0	24/05/2021	Final	Laura Mitchell	Director of Information and Records Services	Approved
3.0	05/01/2022	Final	Andy Purkiss	Information Risk & Governance Specialist	Approved
4.0	16/05/2023	Final	John Simmons	Head of Information Governance	Annual review. Update of document control tables

Approval

Version Number	4.0
Approved By	Director of Information and Records Services
Date of Approval	16/05/2023

Review

Review Frequency	Annual
Next Review Date	16/05/2024

Distribution
This version has been circulated to:

	Method	Date
All staff	ISMS intranet page	05/20223

Amendment Suggestion
If you have suggested amendments please make them to **Information Governance Team**

Table of Contents

1. Introduction

1.1 At National Records of Scotland (NRS) we take our customers' trust and right to privacy seriously. We are committed to ensuring that whenever we process personal data we do so fairly, lawfully and in a transparent manner, and in compliance with data protection and privacy laws, including the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018).

1.2 The UK GDPR provides a framework of rights and duties for the protection of personal data. It sets out the key principles, rights and obligations for most processing of personal data in the UK, and strengthens and extends individuals' rights and protections.

1.3 The DPA 2018 sits alongside and supplements the UK GDPR. It strengthens, or provides exceptions from, some of the requirements of the UK GDPR, and extends data protection laws to processing for law enforcement purposes.

1.4 NRS is committed to ensuring that all of our employees comply with their obligations under the UK GDPR and the DPA 2018 and to safeguarding the integrity and confidentiality of any personal data held or processed by us.

1.5 Our priority will always be to ensure that the rights and freedoms of individuals are protected before we carry out any processing of personal data. Employees should be aware that failure to comply with data protection laws not only risks infringing the rights of individuals, but may also result in loss of reputation, loss of public and stakeholder trust, substantial fines and criminal proceedings against the organisation and individual employees who remain responsible and liable for their actions.

2. Purpose and Scope

2.1 The purpose of this policy is to set out our obligations under data protection laws, demonstrate our commitment to compliance with these, and explain the measures we have put in place in order to achieve this.

2.2 The policy aims to fulfil the requirement for the fair, lawful and transparent processing of all personal data, both in the records which NRS creates and receives in the course of carrying out its functions and administering its own business, and also in the records of organisations and private individuals deposited with NRS for historical purposes.

2.3 The policy relates to all staff and applies to all personal data held by NRS, as defined in the UK GDPR regardless of format or medium, including paper, electronic, audio, visual, microform and photographic.

3. Data Controllers

3.1 The Data Controllers for NRS are the Registrar General of Births, Deaths and Marriages for Scotland and the Keeper of the Records of Scotland. These offices are both held by the NRS Chief Executive Officer.

4. Data Protection Principles

4.1 Article 5 of the UK GDPR sets out six principles relating to the processing of personal data which NRS must be able to demonstrate compliance with. 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 UK 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.

5. Definitions of Personal Data

5.1 Personal data are information that relates to an identified or identifiable living individual.

5.2 The UK GDPR definition of what constitutes personal data includes a wide range of personal identifiers, reflecting current uses of technology and the way organisations collect information about people. For example, online identifiers like IP addresses can be personal data.

"Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

5.3 The UK GDPR uses the term ‘special categories of personal data’ for personal data that is considered to be sensitive' and defines this as:

"… personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and … genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. ..."

Article 9(2) of the UK GDPR provides exemptions under which the processing of special category data is permissible.

6. Personal data processed by NRS

NRS processes personal data and some special categories of personal data. This processing is done in compliance with UK GDPR.

6.1 NRS processes personal data in order to:

- administer public and government services
- maintain accounts and records
- support and manage our staff
- enumerate the census
- produce statistics
- carry out and facilitate research
- manage archives
- administer civil registration
- provide a health administration service
- promote our goods and services

- administer membership records
- assist crime prevention and prosecution of offenders (including CCTV)
- administer information and databanks
- provide consultancy and advisory services

6.2 NRS processes the following categories of personal data:

- personal details – e.g. name, address, etc
- family, lifestyle and social circumstances
- financial details
- employment details
- education and training details
- personal identifiers – e.g. identification numbers, online identifiers

6.3 NRS processes the following special categories of personal data:

- criminal proceedings, outcomes and sentences
- offences (including alleged offences)
- physical or mental health
- political opinions
- racial or ethnic origin
- religious beliefs
- sexual life
- trade union membership

6.4 NRS processes personal data about the following categories of individuals:

- business contacts
- customers and clients
- individuals featured in archival records
- persons enumerated in Scotland
- suppliers
- members of the public who use our services
- offenders and suspected offenders
- patients
- staff, including volunteers, agents, temporary and casual workers
- students and pupils

7. Lawfulness of processing

7.1 The lawful bases NRS usually relies on to process personal data are:

- Article 6(1)(c) of the UK GDPR – processing is necessary for compliance with a legal obligation to which the Registrar General or Keeper are subject

- Article 6(1)(e) of the UK GDPR – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Registrar General or Keeper

8. Policy Statement and Commitment

8.1 In order to fulfil our obligations under data protection law NRS is committed to:

- making data subjects aware of when we collect personal data about them, and explaining the ways in which that information will be used;
- making data subjects aware of their rights and how they can exercise them;
- ensuring that there is a lawful basis for any processing;
- ensuring that processing is fair and will not be unduly detrimental, unexpected or misleading to individuals;
- processing personal data which are adequate, relevant and limited to what is necessary for the intended purposes;
- ensuring that, where necessary, reasonably expected and achievable, personal data are accurate and kept updated;
- retaining personal data only for as long as they are needed;
- taking appropriate technical and organisational measures to safeguard the integrity and confidentiality of personal data;
- ensuring that personal data are not transferred outside the EEA without appropriate safeguards;
- maintaining records of processing activities and organisational compliance.

With exemptions, where appropriate, for personal data which are processed only for public interest archiving, statistical purposes, or historical research purposes.

8.2 This is achieved through:

- use of appropriate privacy notices and privacy information to inform data subjects wherever the collection and processing of personal data takes place, outlining the purposes for which the data will be used, who it will be shared with, how it will be securely retained, and how individuals may access it;
- quick and efficient handling of subject access requests and other information rights requests;
- identification of a Data Protection Officer with specific operational responsibility for data protection in NRS;
- board level oversight, by the Executive Management Board (EMB), of data protection policies and procedures;
- training all NRS staff in data protection and information management in order to ensure that they understand their obligations;

- operation and regular review of comprehensive procedures for the management and security of all NRS information, regardless of media or format;
- maintenance of an information asset register and records of processing activities;
- appropriate monitoring, review and audit of the personal data collected, stored and used by NRS;
- active use of retention and disposal schedules to ensure that information is only retained for as long as it is required;
- ensuring individuals are aware of their obligations when being given access to personal data for research purposes;
- sharing information lawfully and in accordance with the Information Commissioner's Office Data Sharing Code of Practice; entering into data sharing agreements with third parties, which clearly state the terms under which information will be shared;
- entering into data processing agreements whenever NRS processes personal data on behalf of another data controller, or where NRS contracts data processing services;
- assessing the need for, and as appropriate, conducting Data Protection Impact Assessments for the processing of personal data to ensure the processing is appropriate, proportionate, and the rights of the individual are upheld;
- as appropriate engaging and consulting with the Information Commissioner's Office directly on policy and process discussions touching on privacy, data sharing and other data protection issues;
- notifying the Information Commissioner's Office of any reportable personal data breaches within 72 hours of becoming aware of the incident and notifying individuals where there is a high risk to their rights and freedoms;
- ensuring that the suppliers and third parties we instruct to process personal data comply with this policy and data protection requirements.

9. Roles and Responsibilities

9.1 All staff within NRS must comply with the principles set out in this policy. Breaches of this policy and therefore data protection laws may lead to disciplinary action, in line with Scottish Government's 'Civil Service Code' and associated disciplinary procedures. Colleagues must familiarise themselves with, and follow this policy, ensure that procedures for the collection and use of personal data are complied with in their area, and familiarise themselves with the implications of data protection for their role.

9.2 The NRS Chief Executive, who holds the offices of the Registrar General and the Keeper, has primary responsibility for ensuring that all collection and

processing of personal data within the organisation complies with the data protection laws and principles.

9.3 The NRS Data Protection Officer, supported by the NRS Information Governance Team, has responsibility for identifying and publicising responsibilities for data protection within NRS, in accordance with this policy.

9.4 Senior management regard the lawful and correct treatment of personal data as of vital importance to the success of our business operations, and to maintaining the confidence of our stakeholders. Senior management will make provision for a regular review of this policy.

9.5 The NRS Information Governance Team will:

- ensure that this policy and other internal policies relating to data protection are kept up to date,
- provide advice, guidance, training and support to staff to help ensure that they comply with their obligations under the data protection laws,
- ensure the information asset register and records of processing activities are maintained.

9.6 Line managers must ensure all their staff adhere to this policy and data protection principles when performing their duties, and complete mandatory data protection training annually.

10. Monitoring and Review

10.1 Compliance with this policy and related standards and guidance will be monitored by the NRS Data Protection Officer and NRS Information Governance Team, in consultation with the NRS Chief Executive, NRS Executive Management Board and NRS Information Security Committee.