Policy for Processing Special Categories of Personal Data and Personal Data Relating to Criminal Convictions and Offences

Approval date:	**12 September 2022**
Version number:	**1.0**
Author:	**David Morgan, IG Manager, FOI Lead and DPO – reviewed and adapted with permission from an original by Adam Panagiotopoulos, Information Governance Adviser, NSS, Digital and Security**
Review date:	**12 September 2022**
Security classification:	**OFFICIAL – Green: unclassified information**

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

Document reference number: HRPOL043

NHS Shetland Document Development Coversheet*

Name of document	Policy for Processing Special Categories of Personal Data and Personal Data Relating to Criminal Convictions and Offences		
Document reference number	HRPOL043	**New or Review?**	New
Author	David Morgan, Head of IG, FOI Lead and DPO – adapted with permission from an original by Adam Panagiotopoulos, Information Governance Adviser, NSS, Digital and Security		
Information Asset Owner	David Morgan, Head of IG, FOI Lead and DPO		
Executive lead	Colin Marsland, Director of Finance and SIRO		
Review date	12 September 2025		
Security classification	Official – Green: unclassified information		

Proposed groups to present document to:		
IGSG	DISG	CGC

Date	**Version**	**Group**	**Reason**	**Outcome**
11/05/2021	0.1	IGSG	PO	PRO
04/04/2022	0.3	DISG	PO	PRO
12/09/2022	0.4	CGC	FA	A

Examples of reasons for presenting to the group	**Examples of outcomes following meeting**
Professional input required re: content (PI)	Significant changes to content required – refer to Executive Lead for guidance (SC)
Professional opinion on content (PO)	To amend content & re-submit to group (AC&R)
General comments/suggestions (C/S)	For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)
For information only (FIO)	Recommend proceeding to next stage (PRO)
For proofing/formatting (PF)	For upload to Intranet (INT)
Final Approval (FA)	Approved (A) or Not Approved, revisions required (NARR)

***To be attached to the document under development/review and presented to the relevant group**

Please record details of any changes made to the document in the table below

Date	Record of changes made to document
11/05/2021	NSS document (titled ‘Appropriate Policy Document when processing special categories of personal data and personal data relating to criminal convictions and offences’) adapted for NHS Shetland by David Morgan and saved as version 0.1
23/06/2021	Edits made by Sam Collier-Sewell, Senior IG Officer to ensure compliance with NHS Shetland document standards and consistency with local policy framework. Saved as version 0.2
17/03/2022	Changed policy title from ‘Information Processing Policy’. Saved as version 0.3
29/08/2022	RIC added – saved as version 0.4
12/09/2022	Approved at CGC with no changes. Saved as version 1.0

Contents

1. Introduction and background

1.1. This document is adapted with permission from the National Services Scotland (NSS) ‘Appropriate Policy Document (when processing special categories of personal data and personal data relating to criminal convictions and offences)’

1.2. Shetland Health Board (hereinafter referred to as NHS Shetland) processes special categories of personal data and personal data relating to criminal convictions and offences (hereinafter ‘criminal offence data’) in accordance with the UK General Data Protection Regulation (UK-GDPR) and the Data Protection Act 2018 (DPA 2018). Unless otherwise indicated, the reference to ‘personal data’ in this document covers both the special categories of personal data and criminal offence data that NHS Shetland processes.

1.3. Under Schedule 1 of the DPA 2018, NHS Shetland is required to have an appropriate policy document (APD) in place which:

a. explains NHS Shetland procedures for securing compliance with the principles in Article 5 UK-GDPR in connection with the processing of personal data in question; and

b. explains NHS Shetland policies as regards the retention and erasure of personal data processed, giving an indication of how long such personal data is likely to be retained.

1.4. NHS Shetland is also required under the DPA 2018 to

a. retain the APD (this policy);

b. review and, if appropriate, update it; and

c. make it available to the Information Commissioner (ICO), on request, without charge.

1.5. This policy:

a. covers all staff who work for or under contract to NHS Shetland, including contractors, students, agencies, bank staff, volunteers, job applicants, patients, donors, users of NHS Shetland services and products and NHS Shetland customers;

b. supplements and should be read in conjunction with other NHS Shetland policies and documents in force from time to time, such as the NHS Shetland Data Protection Policy, and with any other privacy notice we may provide on specific occasions when NHS Shetland is collecting or using personal data;

c. also applies to NHS Shetland data processing where an APD is not required under the DPA 2018;

d. does not apply to processing special categories of data or criminal offence data for law enforcement purposes. The Policy for Processing Special Categories of Personal Data for Law Enforcement Purposes covers data processing operations that are carried out with the primary purpose of law enforcement;

e. will be reviewed every two years or revised more frequently if necessary, in light of any changes in the underlying legal, regulatory and policy frameworks and business operations and tasks;

f. will be retained for the duration of our processing and for a minimum of 6 months after processing ceases;

2. Personnel responsible for this policy

2.1. The Senior Information Risk Owner (SIRO) has overall responsibility for the effective operation of this policy.

2.2. All staff are responsible for abiding by this policy.

2.3. If you have any questions regarding this policy please contact the NHS Shetland Data Protection Officer (DPO) at shet.dpo@nhs.scot or by calling Montfield Headquarters on 01595 743060.

3. Special categories of personal data and criminal offence data processing at NHS Shetland

3.1. Special categories of personal data are defined in Article 9 UK-GDPR and Section 35 (9) DPA 2018 as personal data revealing:

- Racial or ethnic origin
- Political opinions[1]
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person’s sex life or sexual orientation

3.2. The processing of personal data relating to criminal convictions and offences is regulated in Article 10 UK-GDPR. In addition, Section 11(2) of the DPA 2018 states that this data category includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing.

4. UK-GDPR conditions for processing special categories of personal data

4.1. We process special categories of personal data under the following UK-GDPR Articles:

a. **Article 9(2)(b)** – employment, social security or social protection.

Data processing is necessary for the purposes of carrying out the obligations and exercising specific rights of NHS Shetland or of the data subject in the field of

[1] NHS Shetland does not systematically process staff personal data relating to political opinions.

employment and social security and social protection law. Examples of our processing include staff sickness absences and political activity declarations.

b. **Article 9(2)(h)** –for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

   Examples of our processing include the processing of personal data as part of the provision of community and hospital healthcare services such as District Nursing, General Practice, Dentistry, Community Mental Health Services and Hospital Services as well as the management and provision of occupational health service to staff.

c. **Article 9(2)(j)** – for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

   Examples of our processing include the data transfers to the Shetland Archives in accordance with our obligations under the Public Records (Scotland) Act 2011.

d. **Article 9(2)(f)** – for the establishment, exercise or defence of legal claims

   Examples of our processing include processing relating to any employment tribunal or other litigation.

e. **Article 9(2)(g)** – reasons of substantial public interest

   Data processing of personal data is necessary for the purposes of substantial public interest to carry out our duties and tasks in line with National Health Service (Scotland) Act 1978 (the 1978 Act) and other applicable frameworks.

f. **Article 9(2)(i)** – processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices

   Examples include data processing for monitoring and managing public health crises.

g. **Article 9(2)(c)** – vital interests of the data subject or of another individual where the data subject is physically or legally incapable of giving consent

   Examples of our processing include using health information about a member of staff in a medical emergency.

h. **Article 9(2)(a)** – explicit consent

   In exceptional circumstances we may seek the explicit consent of individuals only where it can meet the legal requirements.

4.2. More information about the applied legal bases will be published in the relevant data protection (privacy) notices.

5. UK-GDPR conditions for processing criminal offence data

5.1. We process criminal offence data under Article 10 UK-GDPR and Section 11 DPA 2018. Examples of our processing of criminal offence data include pre-employment checks, fraud prevention checks and declarations by an employee in line with contractual obligations.

5.2. More information about the applied legal bases will be published in the relevant data protection (privacy) notices.

6. Schedule 1 DPA 2018 conditions for processing special categories of personal data

6.1. We may process special categories of personal data for the following purposes in line with Part 1 of Schedule 1:

a. **Paragraph 1** Employment, social security and social protection.

6.2. We may process special categories of personal data for the following purposes in Part 2 of Schedule 1.

a. **Paragraph 6** Statutory etc. and government purposes

b. **Paragraph 8** Equality of opportunity or treatment

c. **Paragraph 9** Racial and ethnic diversity at senior levels of organisations

d. **Paragraph 10** Preventing or detecting unlawful acts

e. **Paragraph 11** Protecting the public against dishonesty

f. **Paragraph 12** Regulatory requirements relating to unlawful acts and dishonesty

g. **Paragraph 14** Preventing fraud

h. **Paragraph 15** Suspicion of terrorist financing or money laundering

i. **Paragraph 18** Safeguarding of children and of individuals at risk

j. **Paragraph 24** Disclosure to elected representatives

7. Schedule 1 DPA 2018 conditions for processing criminal offence data

7.1. We may process criminal offence data for the following purposes in parts 1, 2 and 3 of Schedule 1:

a. **Paragraph 1** Employment, social security and social protection

b. **Paragraph 6** Statutory etc. and government purposes

c. **Paragraph 10** Preventing or detecting unlawful acts

d. **Paragraph 11** Protecting the public against dishonesty

e. **Paragraph 12** Regulatory requirements relating to unlawful acts and dishonesty etc

f. **Paragraph 14** Preventing fraud

g. **Paragraph 15** Suspicion of terrorist financing or money laundering

h. **Paragraph 33** Legal claims

8. Procedures for securing compliance

8.1. At NHS Shetland, we are committed to safeguarding and protecting personal data and using it in accordance with the applicable data protection framework. More specifically, NHS Shetland will take all the appropriate measures to respect the following principles when processing personal data:

a. Lawfulness, fairness and transparency

NHS Shetland will use your personal information lawfully, fairly and in a transparent way. NHS Shetland will put in place appropriate technical and organisational measures to meet the requirements of lawfulness, fairness and transparency. These will include:

i. Processing personal data only where an appropriate legal basis is established before data processing takes place.

ii. NHS Shetland will rely on clearly defined legal bases in line with its public remit and statutory duties to support the delivery of health and care services. Personal data will be processed in accordance with the applicable regulatory framework under which NHS Shetland operates as an NHSS organisation and in relation to its public duties and functions.

iii. The processing of special categories of personal data and criminal offence data will take place only where strictly necessary.

iv. Keeping data subjects informed about the processing of their personal data through publically available data protection (‘privacy’) notices and this policy. Privacy notices covering specific uses of personal data may be also provided directly to the data subjects.

b. Purpose limitation

NHS Shetland will process personal information only for specified, explicit and legitimate purposes that we have clearly explained and not used in any way that is incompatible with those purposes or could breach the data subjects’ expectations. We will put in place appropriate technical and organisational measures to meet the requirements of purpose limitation. These will include:

i. NHS Shetland will lawfully process personal data collected for the stated purposes as specified in the privacy notices, providing that the processing is necessary and proportionate to these purposes.

ii. NHS Shetland will keep this information up to date and conducts regular reviews and audits to ensure the respect of the purpose limitation principle.

iii. NHS Shetland will not process personal data for purposes incompatible with the original purpose it was collected for.

iv. Where personal data are processed for secondary compatible purposes, NHS Shetland will comply with its data protection obligations, including transparency and the requirement for appropriate safeguards.

v. If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.

c. Data minimisation

NHS Shetland will use personal information that is adequate, relevant and limited to what is necessary in relation to the specific purposes stated in the relevant privacy notices. NHS Shetland will put in place appropriate technical and organisational measures to meet the requirements of data minimisation. These will include:

i. NHS Shetland will collect and process the strictly necessary personal data only to the extent that it is needed to carry out its functions as a public authority, fulfil its operational needs or to comply with any legal requirements.

ii. NHS Shetland will not collect data that are not relevant or proportionate to the stated processing purposes.

iii. NHS Shetland will carefully assess the nature, type and amount of the necessary personal data, especially in relation to special categories of personal data.

iv. Where personal data are not necessary, no personal data will be collected.

v. NHS Shetland will implement appropriate controls and measures to anonymise personal data in order to minimise any risks to data subjects, where necessary and possible.

vi. Where NHS Shetland can perform its tasks efficiently with pseudonymised data, NHS Shetland will apply security and organisational measures to pseudonymise personal data.

vii. NHS Shetland will apply appropriate security measures to all classifications of data.

viii. Where personal data are provided to us or obtained by us, but are not relevant to our stated purposes, we will dispose of it securely and notify the sender of their error or data service requirements.

d. Accuracy

NHS Shetland will take all reasonable and necessary steps to ensure that personal information is accurate and up to date. NHS Shetland will put in place appropriate technical and organisational measures to meet the requirements of accuracy. These will include:

i. NHS Shetland will regularly review the Information Asset Register and our Record of Processing Activities (ROPA) to comply with the accuracy principle.

ii. Data subjects may contact NHS Shetland to provide updated personal data, where relevant. Where personal data are not provided by data subjects, the sources of this data may contact NHS Shetland for the appropriate updates.

iii. Where NHS Shetland becomes aware that personal data are inaccurate or out of date, having regard to the purpose for which data are processed, NHS Shetland will take every reasonable step to ensure that data are rectified without delay.

iv. NHS Shetland will have clear internal policies and allocated responsibilities to communicate and implement any requests to rectify personal data.

v. Where the above is not possible, NHS Shetland will justify and document its decision and inform data subjects.

e. Storage limitation

NHS Shetland will keep personal data only as long as necessary for the specific purposes of data processing as detailed in the relevant privacy notices. NHS Shetland will put in place appropriate technical and organisational measures to meet the requirements of storage limitation. These include:

i. NHS Shetland will keep personal information in accordance with the NHS Shetland Records Management Policy and the Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020.

ii. The NHS Shetland Records Management and Information Security policies will provide for the appropriate retention, and thereafter disposal, of personal data that are no longer required by NHS Shetland and are authorised by the data owner to be disposed of securely.

iii. NHS Shetland will determine the retention period for this data in line with its legal and regulatory obligations and public tasks.

iv. NHS Shetland will document and regularly review the applied retention periods.

v. NHS Shetland will provide data subjects with information about the applied retention periods.

vi. Once no longer needed, personal data will be disposed of securely or rendered permanently anonymous, where this is necessary and possible.

vii. Our retention policy and schedule will be reviewed regularly and updated when necessary.

viii. NHS Shetland will have appropriate policies for reviewing and auditing where personal data have been disposed of or anonymised, upon the completion of the applied retention period, where necessary.

ix. NHS Shetland will have appropriate policies for securely disposing of physical and electronic copies of personal data.

f. Integrity and confidentiality

NHS Shetland will keep and process personal data securely to protect it against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. NHS Shetland will put in place appropriate technical and organisational measures to meet the requirements of integrity and confidentiality. These will include:

i. The NHS Shetland Information Security Policy and associated Policies which provide safeguards for data confidentiality, integrity and availability.

ii. Electronic information will be processed within our secure network.

iii. Hard copy information will be kept secure at all locations (including offices, home and archival storage locations) and processed and disposed of in line with our security procedures.

iv. Our electronic and physical storage systems will have appropriate access controls and audit logs applied.

v. Authorised staff will only have access to personal data on a need-to-know basis, as required by their business role, and this access will be reviewed periodically.

vi. We will have information security policies and systems to monitor and remedy any compromise of data security.

vii. Third parties or contractors with which NHS Shetland engages will only process personal information on our instructions or with our agreement, and where they do so, they will agree to treat the information confidentially and to keep it secure.

g. Accountability

NHS Shetland will be able to demonstrate its compliance with data protection law and its obligations under the UK-GDPR and the DPA 2018 and other applicable data protection requirements. NHS Shetland will put in place appropriate technical and organisational measures to meet the requirements of accountability. These will include:

i. Appointing a Data Protection Officer (DPO) who will report directly to our highest management level.

ii. Appointing a Senior Information Risk Owner (SIRO), Information Security Officer (ISO), Caldicott Guardian, Information Asset Owners (IAOs) and Information Asset Administrators (IAAs).

iii. Establishing an internal, dedicated team of Information Governance experts responsible for ensuring and monitoring NHS Shetland’s compliance with data protection law and best information governance practices.

iv. Keeping documentation of NHS Shetland data processing activities up to date.

v. Adopting and implementing training, policies and associated documentation in relation to the use, access and protection of personal data to establish a robust organisational data protection culture.

vi. Applying the appropriate security measures and keeping up-to-date documentation about these organisational and technical measures.

vii. Having appropriate privacy notices in place and making them available when required.

viii. Ensuring that our external partners and contractors comply with data protection law and implementing data processing agreements with them.

ix. Conducting data protection and security data protection impact assessments, where required, and keeping these up to date.

x. Conducting risk assessments as proactive risk mitigation measures.

xi. Taking a ‘data protection by design and default’ approach to our activities.

9. NHS Shetland’s policies for retention and erasure of personal data

9.1. NHS Shetland will ensure that, where special category or criminal convictions personal data are processed:

a. There is a record of that processing, and that record will set out, where possible, the envisaged time limits for disposal of the different categories of data.

b. When no longer required for the purpose for which it was collected and, where necessary and possible, personal data will be securely deleted or rendered permanently anonymous.

c. Data subjects will receive information about how their data will be processed in line with Articles 12-14 UK-GDPR.

9.2. Our retention and disposal practices are set out in the NHS Shetland Records Management Policy and will comply with the Scottish Government Records Management Health and Social Care Code Of Practice (Scotland) 2020

End of document

Appendix 1 – Rapid Impact Checklist

An Equality and Diversity Impact Assessment Tool:

Which groups of the population do you think will be affected by this proposal?* All groups will be affected as the policy relates to the processing of all special category personal data and criminal offence personal data by NHS Shetland. **Other groups:** • Minority ethnic people (incl. Gypsy/travellers, refugees & asylum seekers) **Yes** • Women and men **Yes** • People with mental health problems **Yes** • People in religious/faith groups **Yes** • Older people, children and young people **Yes** • People of low income **Yes** • Homeless people **Yes** • Disabled people **Yes** • People involved in criminal justice system **Yes** • Staff **Yes** • Lesbian, gay, bisexual and transgender **Yes** *the word proposal is used as shorthand for the policy, procedure, strategy or proposal that is being be assessed	
In the following sections, please consider what positive and negative impacts you think there may be and which specific groups will be affected by these impacts?	
What impact will the proposal have on lifestyles? For example, will the changes affect: • Diet and nutrition • Exercise and physical activity • Substance use: tobacco, alcohol and drugs • Risk taking behaviour • Education and learning or skills	None

Will the proposal have any impact on the social environment? Things that might be affected include: • Social status • Employment (paid or unpaid) • Social/Family support • Stress • Income	None
Will the proposal have any impact on the following? • Discrimination? • Equality of opportunity? • Relations between groups? • Fairer Scotland Duty	As the policy is intended to ensure the fair and lawful processing of personal data, it is expected that there will be positive impact on the groups noted above.
Will the proposal have an impact on the physical environment? For example, will there be impacts on: • Living conditions? • Working conditions? • Pollution or climate change? • Accidental injuries or public safety? • Transmission of infectious disease?	None
Will the proposal affect access to and experience of services? For example: • Health care • Transport • Social services • Housing services • Education	No impact

Summary Sheet

Positive Impacts (Note the groups affected) Clear guidelines on the processing of special category personal data and personal data relating to criminal convictions should result in the fair and lawful processing of the data of all the groups noted above.	**Negative Impacts (Note the groups affected)** None
Additional Information and Evidence Required None	
Recommendations None	
From the outcome of the RIC, have negative impacts been identified for race or other equality groups? Has a full EQIA process been recommended? If not, why not? No negative impact identified	

Signature(s) of Level One Impact Assessor(s): David Morgan

Date: 29 August 2022