Data Protection

Policy, 2025

Purpose and Scope

This policy has been produced to set out the Trust's responsibilities in relation to data protection law; to outline the key principles; to provide high level guidance on data protection compliance; and to identify associated procedures and guidance to help support compliance.

It is the responsibility of all volunteers and employees to familiarise themselves with this policy and its associated guidance and procedures.

All data protection queries should be directed to the Data Protection team at dataprotection@nts.org.uk

Version Control					
Rev. no.	**Author**	**Date**	**Changes**	**Approved by**	**Published Date**
1.0	Ava Wieclawska	15 October 2018	N/A	ExCo	November 2018
2.0	Ava Wieclawska	06 February 2025	Removal of references to TrustNET and to DPIGG	DPO	February 2025

1. Introduction

The National Trust for Scotland (the Trust), as a Data Controller, is committed to protecting all personal data it processes; carrying out its functions in accordance with data protection laws, including the General Data Protection Regulation (GDPR), UK GDPR, Data Protection Act 2018 and the Privacy and Electronic Communications Regulations (PECR); and in line with the highest standards of conduct.

This policy covers all data processing[1] activities carried out by the Trust's employees, volunteers, contractors and third parties; and all methods of processing personal data including in manual paper records, electronic filing systems (e.g. shared drives/SharePoint

[1] Any operation performed on personal data, including the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

sites), audio and visual recording systems, websites and core databases and systems (including email).

Personal data can be defined as any information relating to an identifiable person (known as a data subject) who can be directly or indirectly identified from that data. For example, name, identification number, location data or online identifier. Personal data that has been pseudonymised (e.g. key-coded) can fall within the scope of personal data depending on how difficult it is to attribute the pseudonym to an individual.

Special Category Data is particularly sensitive personal data that requires careful handling and includes data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

The Trust is fully committed to data protection compliance, and expects all employees, volunteers, contractors and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

2. Data protection principles

The UK GDPR sets out six core principles, as well as an overarching accountability principle, to govern the processing of personal data:

Principle a: Lawfulness, fairness and transparency - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

This means the Trust must:

- *have a lawful basis[2] for processing personal data*
- *process personal data fairly and not unexpectedly*
- *provide privacy information to data subjects at the point of collection or as soon as possible (within one month at the latest) if collected from a source other than the individual themselves*

The Trust will demonstrate compliance with this principle by:

- *ensuring that the correct lawful basis is identified and recorded within our Information Asset Register (Record of Processing Activities)*
- *informing data subjects what processing will be carried out in our Privacy Policies and associated privacy notices*
- *ensuring that the processing carried out by the Trust matches the description given to the data subject*
- *that we appropriately record and obtain consent when relying on consent as the most appropriate lawful basis for processing*

[2] Please see Article 6 of the General Data Protection Regulation for the available lawful bases for processing personal data. If processing special category data, there should also be an Article 9 condition.

Principle b – Purpose limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

This means the Trust must:

- *have clear purposes for processing*
- *regularly review the purposes*
- *check the compatibility and lawful basis of any new purposes*

The Trust will demonstrate compliance with this principle by:

- *being clear in our Privacy Policies and privacy notices about exactly what the personal data collected will be used for*
- *carrying out Data Protection Impact Assessments (DPIAs) for any new processing activities that involve a risk to data subjects*
- *checking our lawful basis and consents preferences prior to further processing of data*
- *informing data subjects if new processing activities are being carried out*

Principle c – Data minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

This means the Trust must:

- *collect and process enough data to fulfil the purposes*
- *collect and process relevant data*
- *not process excessive data*

The Trust will demonstrate compliance with this principle by:

- *collecting and processing data with data minimisation in mind*
- *identifying the minimum data required and not collecting excessive data*
- *using methods of pseudonymisation[3] and anonymisation where appropriate*
- *regularly reviewing the data held and ensuring excessive data is not retained*

Principle d - Accuracy: Personal data shall be accurate and kept up to date.

This means the Trust must:

- *take reasonable steps to ensure the accuracy of data held*
- *ensure that there are clear and consistent processes in place for updating records*
- *consider any challenges to the accuracy of data*

The Trust will demonstrate compliance with this principle by:

- *adopting clear Privacy Management Procedures for the updating of personal data*

[3] Data amended in such a way that individuals can no longer be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.

- *ensuring that audit trails are held of any data changes*
- *utilising data quality checks on data entry, where possible (e.g. postcode look-ups)*

Principle e – Storage limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

This means the Trust must:

- *consider the purposes for processing data when assessing suitable retention periods*
- *only retain personally identifiable information for as long as necessary*
- *adopt suitable technical and organisational measures to prevent the reidentification of deidentified data subjects*

The Trust will demonstrate compliance with this principle by:

- *applying retention policies to personal data held (with review mechanisms and holds);*
- *removing duplicate data wherever possible*
- *ensuring that records are irretrievably deleted or transferred to the archives at the end of their retention period*

Principle f - Integrity & Confidentiality: Personal data shall be 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.

This means the Trust must:

- *use appropriate technical and organisational measures to protect personal data*
- *ensure the confidentiality, integrity and availability of systems and services*
- *restore access in the event of a physical or technical incident*
- *adopt processes to effectively test measures and make improvements*

The Trust will demonstrate compliance with this principle by:

- *deploying state of the art security controls*
- *adopting clear policies and procedures in relation to information security and governance*
- *regularly reviewing information and security risks*

Principle – Accountability: The Data Controller shall be responsible for, and be able to demonstrate compliance with the principles.

This means the Trust must:

- *evidence our lawful basis for processing*
- *explain why we process personal data*
- *demonstrate how we comply with the principles*
- *document our processing activities*

The Trust will demonstrate compliance with this principle by:

- *developing a governance framework for data protection, consisting of key policies and procedures*
- *taking a Data Protection by Design and Default approach to new systems development*
- *ensuring there a data processing contracts in place with all data processors*
- *developing a Record of Processing Activities*

3. Lawful processing

Of the six available lawful bases for processing personal data, the Trust is most likely to rely on contract, legitimate interests, consent and legal obligation. Please refer to the guidance below when identifying the most appropriate lawful basis for new data processing activities.

There must be an additional condition as set out in Article 9 of GDPR when processing special category data and an additional condition when processing data relating to criminal convictions and offences.

Contract

The Trust can identify contract as the most appropriate lawful basis for processing when we need to process personal data to fulfil our contractual obligations to a data subject or because the data subject has asked the Trust to do something before entering into a contract (for example, consider an application form in relation to a vacancy).

It is important to note that the processing must be necessary. If it is possible to do what the data subject has requested without processing any personal data, this basis will not apply. Also, if we want to give some data subjects the ability to opt out of the data processing, this lawful basis will not apply, as the processing is not necessary for the contract.

Legitimate interests

This is the most flexible lawful basis and is likely to apply when a data subject would reasonably expect the Trust to manage their data in a particular way, when the processing will have a minimal privacy impact, or where there is a compelling justification for the processing.

When identifying legitimate interests as the most appropriate lawful basis, the Trust must carry out and evidence a three-part test, known as a Legitimate Interest Assessment[4], to identify the legitimate interest; show that the processing is necessary to achieve it; and balance it against the data subject's interests, rights and freedoms.

If the use of legitimate interests is approved by a relevant senior manager, data subjects must be told in privacy notices what the legitimate interest is.

[4] Please speak to the Data Protection Officer for advice on conducting Legitimate Interest Assessments.

Consent

Consent means offering data subjects real choice and control over how their data is processed. When obtained and managed correctly it can help build real trust and confidence in the data processing activities of the Trust.

When identifying consent as the most appropriate lawful basis for processing, the Trust must present the request for consent in a manner which is clearly distinguishable, in an intelligible and easily accessible form, and using clear and plain language.

Consent must be freely given, cannot be based on a contract that is conditional to the processing of personal data and must be separate from other terms and conditions. The consent request must be based on a positive opt-in and not a pre-ticked or default consent.

For accountability purposes, the Trust must document the date, method and content of the consent given and each time the Trust communicates with a data subject under their consent to do so, it must provide a simple method for the data subject to update their contact preferences or withdraw their consent at any time.

If consent is difficult to obtain and manage, the Trust should consider another lawful basis for processing (for example, legitimate interests).

Legal obligation

The Trust can rely on this lawful basis if we need to process the personal data to comply with a common law or statutory obligation. Please note that the processing must be necessary. If it is possible to do comply with the legal obligation without processing any personal data, this basis will not apply.

4. Privacy Policies and Notices

A key requirement of data protection law is that data subjects are informed about the collection and use of their personal data.

When personal data is collected from a data subject, privacy information must be provided at the point of collection, unless the data subject already has the information, or the provision of information proves impossible or would involve disproportionate effort.

Privacy information can be provided in layers. For example, a first layer privacy notice that contains the following information as a minimum can be provided at the point of collection:

- *the details of the purposes of processing*
- *the identity of the Trust as the data controller*
- *the existence of the rights of the data subject, together with information on the greatest impact of processing or processing which could surprise the data subject*

This first layer notice should then contain a link to a second layer Privacy Policy (available in hard copy, by email or on the Trust's website), containing the remaining Article 13 conditions.

Privacy information must be regularly reviewed, and where necessary, updated. If significant changes are made to privacy information, data subjects must be actively informed of these changes. If we are to use personal data for a new purpose, we must tell the data subject before we begin the new processing activity.

Records of privacy information must be retained, along with a record of the facts, date, content, and method of disclosure.

5. Retention of personal data

Personal data will not be retained by the Trust for longer than necessary in relation to the purposes for which it was processed. The length of time the Trust needs to retain personal data is set out in the *Records Retention Schedule*. This considers legal and contractual requirements as well as legitimate organisational need to retain the data. Personal data should be deleted or destroyed as soon as it has been confirmed that there is no longer a need to retain it.

It is important to note that the Trust must not delete data if there is action being carried out on that data e.g. Data Subject Access Request, complaint, legal action.

6. Protecting personal data

The Trust must adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by human action or the physical environment.

The minimum requirements are detailed within Information Security Policies, and include:

- *Preventing unauthorised persons from gaining access to personal data.*
- *Ensuring that access to personal data is provided on a need-to-know basis.*
- *Securing hard copy records in lockable rooms (restricted to appropriate staff) or in lockable containers.*
- *Ensuring (where necessary) that personal data sent digitally is encrypted or password protected so that it cannot be read, copied, modified or removed without authorisation.*
- *Ensuring that access logs are in place to establish when personal data was entered into, modified on or removed from a system.*
- *Ensuring that in the case where processing is carried out by a Data Processor[5], the data is processed only in accordance with the instructions of the Trust, as set out in a Data Processing Contract[6].*

[5] A third party, processing personal data on behalf of the Trust (e.g. a website provider, a confidential waste contractor etc).

[6] Please speak to the Legal & Governance Manager and Data Protection Officer for advice on these contracts.

- *Ensuring that personal data is protected against corruption, destruction and accidental loss or damage.*

7. Data Protection by Design and Default

Data protection by design is about considering data protection and privacy issues at the design phase of any system, service, product or process and then throughout its lifecycle. It requires the Trust, when considering developing new systems and processes, to put in place appropriate technical and organisational measures to implement the data protection principles and integrate safeguards into the processing activities to protect a data subject's rights.

Data protection by default requires the Trust to only process the data that is necessary to achieve the specific purpose. It means that the Trust must specify what data must be processed, before the processing starts, appropriately inform individuals and only process the data needed for the purpose.

Data Protection Impact Assessments (DPIA)

DPIAs are a tool to help us understand and manage privacy risks in relation to data processing activities. They are an integral part of data protection by design and by default in assessing privacy risks and identifying measures to mitigate such risks at the start of any new project or process involving personal data. For guidance on completing DPIAs, please refer to the *DPIA Policy*.

8. Digital marketing

When sending digital marketing communications to data subjects, the Trust must identify the most appropriate lawful basis for processing and have due regard to all data protection laws as well as any e-Privacy rules.

Digital marketing is not permitted unless the communication has been identified as necessary for a contract (for example, service messages to members) or opt-in consent has been obtained.

Prior to sending digital marketing communications, due diligence must be carried out to ensure that data subjects who have previously objected to such communications are not contacted.

When sending digital marketing messages, data subjects must be given the option to opt-out of any future communications (unless the message is considered necessary as part of the contract) in every communication.

9. Data subject's rights

Data subjects have enhanced rights under data protection laws and the Trust has a responsibility to ensure that all data subjects are aware of their rights and how to exercise them. These rights include:

- *The right to be informed*
- *The right of access*
- *The right to rectification*
- *The right to erasure*
- *The right to restrict processing*
- *The right to data portability*
- *The right to object*
- *The right to not be evaluated on the basis of automated processing*

Please refer to the *Data Subjects Rights Policy* and associated Privacy Management Procedures for further information.

10. International transfers

The UK GDPR restricts the transfer of data outside of the EEA. The Trust may only transfer personal data to recipients outside of the EEA where that country is recognised as having an adequate level of protection for the rights and freedoms of the relevant data subjects, or the appropriate safeguards and an approved transfer mechanism have been identified and agreed[7].

11. Governance and complaints handling

The Trust regards the lawful and correct processing of personal data as a key part of building trust and confidence with our members, donors, external and internal customers.

Data subjects who have a complaint about the processing of their personal data, should be advised to put forward the matter in writing to the relevant Head of Department, who will in turn inform the Data Protection Officer (DPO). An investigation of the complaint will be carried out and the Head of Department will inform the data subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the data subject and the Trust, then the data subject may complain to the Information Commissioner's Office.

12. Breach Reporting

A personal data breach can be defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

If a personal data breach occurs, the member of staff or volunteer who has discovered the breach, must inform the DPO as soon as possible. If it is assessed that the breach is likely to pose a risk to the rights and freedoms of the individuals, the Trust must notify the

[7] For example, appropriate safeguards, International Data Transfer Agreements, Transfer Risk Assessments, Standard Contractual Clauses, Binding Corporate Rules, Codes of Conduct, Certification Mechanisms. Please speak to the Data Protection Officer for further information.

Information Commissioner's Office within 72 hours. If a high risk is likely, the Trust must inform the data subjects without undue delay. Please refer to the *Personal Data Breach Management Policy* and associated *Breach Reporting Procedures* for further information.

13. Compliance monitoring, risk management and review

To confirm that an adequate level of compliance is being achieved and maintained by the Trust, the DPO will liaise with Internal Audit to ensure that frequent compliance audits are being executed. Each audit will, as a minimum, assess:

- *Compliance with this policy in relation to the protection of personal data, including the assignment of responsibilities, raising awareness and training.*
- *The effectiveness of operational practices, including rights, transfers, incident management and complaints handling.*
- *The level of understanding of policies and the use of privacy notices.*
- *The accuracy of personal data being stored, and the recording and accountability of personal data being processed.*

The DPO will also carry out regular compliance checks through the network of Data Champions and will be responsible for identifying and reviewing risks in relation to data protection compliance. Due to the consequences of non-compliance and our aim to build trust in the way we handle personal data, the risk appetite in relation to data protection is low.

This policy will be reviewed annually.