Northern Ireland Policing Board

# NORTHERN IRELAND POLICING BOARD

# DATA PROTECTION POLICY

# Northern Ireland Policing Board

# Data Protection Policy

Implementation Date: August 2021
Review date: August 2023



Record No. 445142

## Introduction

1. A key priority for the Northern Ireland Policing Board (the Board), as a data controller is to protect the rights and privacy of individuals in accordance with the UK's General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

2. Within our directorates, we collect and use personal data in order to carry out our business and provide our services. Our data subjects include members of the public, current, past and prospective employees, clients, customers and suppliers.

3. Our directorates are as follows:

   - Partnership
   - Performance
   - Police Administration
   - Resources

4. The Board has governance and accountability measures in place to ensure that all employees, contractors, agents, consultants and other parties who have access to personal data (including special categories of personal data) held by or on behalf of us are fully aware of and abide by their duties and responsibilities under the legislation.

## Data Protection Principles

5. The Board fully supports and complies with the seven principles of the UK GDPR. In summary, this means personal data will be:

   i. processed lawfully, fairly and in a transparent manner;
   ii. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
   iii. adequate, relevant and limited to what is necessary;
   iv. accurate and, where necessary, kept up to date;
   v. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed;
   vi. 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; and
   vii. Processed in an accountable manner.

## Governance Structure

6. The Board has a strong governance structure in place to safeguard personal data. To demonstrate the Board's commitment, we have:

- a Data Protection Officer to monitor internal compliance and inform and advise on the Board's data protection obligations;
- a Senior Information Risk Owner (SIRO) who takes overall ownership of the organisation's information risk policy and is responsible for ensuring that information risk is managed appropriately;
- Information Asset Owners (IAOs) who are responsible for the secure management of personal data within their business areas. They will ensure any information being disclosed remains secure and will investigate any data security incidents;
- A Records Manager and a Compliance Officer to provide policy and guidance on data protection within the organisation; and
- A reporting structure to the Senior Management Team and the Board's Audit and Risk Management Committee (ARAC) in respect of Data Protection issues.

## Processing of Personal Data

7. The Board will, through appropriate training and responsible management:

- take a data protection by design and default approach to all work to incorporate data protection compliance at an early stage of all projects;
- fully observe conditions regarding the lawful, fair and transparent processing of personal data and special category data;
- maintain appropriate documentation on processing activities;
- provide clear, easily accessible information to inform data subjects about the collection and use of their personal data;
- collect and process personal data only to the extent that it is needed to fulfil operational needs or to comply with legal requirements;
- as far as possible, ensure the quality and accuracy of personal data used;
- apply appropriate data retention schedules to determine the length of time personal data is held;
- ensure that data subjects can fully exercise their rights under the data protection legislation;
- put in place appropriate technical and organisational security measures to safeguard personal data;
- ensure that personal data is not transferred abroad without adequate safeguards; and

- ensure all personal data is held in line with the Board's information management policies, procedures and guidance.

**Compliance**

8. Our IAOs will ensure that:

   - only staff who need access to personal data as part of their duties are authorised to do so;
   - all staff processing personal data are appropriately trained and supervised; and
   - procedures for handling personal data are clearly understood, available and regularly reviewed.

**Staff Responsibilities**

9. All staff managing and processing personal data are directly and personally responsible for following good data protection and records management practice. They will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss, disclosure or destruction and in particular will ensure that:

   - they are aware of data protection and information management policies, procedures and guidance;
   - the complete data protection training and awareness; and
   - all records and documents containing personal/special category data are processed securely.

10. If and when, as part of their responsibilities, staff process information about other people, they must comply with this policy and their business area's own data handling procedures. Staff must not disclose personal data outside this guidance or use data held on others for their own purposes. Staff should go through the proper subject access rights process for accessing their own personal data.

**Data Breach Management**

11. In the event of a data breach, staff must follow procedures set out in the Board's Security / Data Breach Incident Reporting Policy. The purpose of the policy is to ensure that a consistent and effective approach is applied to handling data incidents. The policy sets out arrangements for the management of incidents and sets out the roles of staff in reporting and investigating breaches.

## Data Sharing

12. Data sharing means the disclosure of information from the Board to a third party organisation or organisations.

13. Before disclosing personal data to another organisation, staff will ensure all sharing is lawful, fair, transparent and in line with the rights and expectations of data subjects.

14. Where the Board engages a data processor, a written contract will be put in place to ensure both parties understand their obligations, responsibilities and liabilities. Any suppliers who are users of personal data supplied by the Board will be required to confirm and demonstrate that they will abide by the requirements of the legislation and the terms and conditions of the contract.

15. Where personal data is shared with another public authority, a data sharing agreement is required to define a common set of rules to be adopted by all parties subject to the data sharing operation.

16. Data sharing agreements and contracts will be drawn up in line with the Board's Guidance on Data Sharing.

## Policy Awareness

17. A copy of this policy will be given to all new members of staff and interested third parties. Existing staff and any relevant third parties will be advised of the policy which will be posted on our website. It may also be made available in other formats on request to the Data Protection Officer.

18. All staff and relevant third parties must be familiar with and comply with this policy at all times. The policy will be reviewed every two years.

## Contact

19. In the event that a data subject has a concern or complaint in relation to the Board's handling of personal data or wishes to exercise their rights under the legislation, they can contact the Data Protection Officer. Data subjects can also complain to us if they are dissatisfied with our response to a subject access request. We aim to respond to complaints or queries within 28 calendar days of receipt of correspondence.

20. The Data Protection Officer can be contacted as follows:

Data Protection Officer
Northern Ireland Policing Board
Waterside Tower
31 Clarendon Road
Clarendon Dock
Belfast
BT1 3BG
Email: Data.protection@nipolicingboard.org.uk
Telephone: 028 90408500

21. Data subjects also have the right to lodge a complaint directly with the Information Commissioner at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113
Email: casework@ico.org.uk
Website: https://ico.org.uk/make-a-complaint/your-personal-information-concerns/

**Northern Ireland Policing Board**
Waterside Tower
31 Clarendon Road
Clarendon Dock
Belfast BT1 3BG

**028 9040 8500**

**information@nipolicingboard.org.uk**

**www.nipolicingboard.org.uk**

**policingboard**

**@nipolicingboard**

**nipolicingboard**

**Northernirelandpolicingboard**

**DOCUMENT TITLE**

**Northern Ireland Policing Board**
**Data Protection Policy**
**August 2021**

**ONLINE FORMAT**

This document is available in PDF format from our website. This document may also be made available upon request in alternative formats or languages. Requests should be made to the Northern Ireland Policing Board.