NEIGHBOURHOOD WATCH NETWORK

DATA PROTECTION POLICY

Author: Sandra Bauer

Approved: March 2026

Next review due: March 2029

1. Purpose

1.1 This policy forms part of Neighbourhood Watch Network's commitment to the safeguarding of personal data processed by staff, volunteers, Multi Scheme Administrators (MSAs), and Trustees. The aim of this policy is to clarify the rights and obligations of NWN staff, volunteers MSAs and Trustees with respect to personal data.

1.2 This policy is supported by sub-policies that include greater detail on specific aspects of data management and security. The sub-policies cover (to view these please contact us):

- Data Retention Schedule
- Subject Access Requests
- Data Breaches
- Privacy Notice
- Volunteer Privacy Notice
- Staff Privacy Notice
- Job Applicant Privacy Notice

2. Introduction

2.1 Neighbourhood Watch Network processes the personal data of individuals including staff, Trustees, volunteers, members and stakeholders, and including partners and funders. This processing is regulated by the Data Protection Act 2018, the General Data Protection Regulation 2018 (GDPR) and the Fundraising Regulator Code of Practice 2025.

3. Scope

3.1 This policy applies to all Neighbourhood Watch Network staff, MSAs[1], other volunteers and Trustees.

3.2 Key changes to the policy have been introduced during 2025 and are contained within **Appendix 1** it will make some changes to them to make the rules simpler for organisations, encourage innovation, help law enforcement agencies to tackle crime and allow responsible data-sharing while maintaining high data protection standards.

4. Data Protection Act

[1] This is introduced and explained during MSA training modules and online training events.

4.1 This Data Protection Policy follows the requirements of the Data Protection Act 2018. The Act aims to promote high standards in the handling of personal information and so protect the individual's right to privacy.

5. Data Protection Principles

5.1 Neighbourhood Watch Network fully endorses and adheres to the principles of Data Protection, as outlined in the Act.

These are that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- 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.
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 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.
- 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.
- 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.
- 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.

6. Individuals' rights

6.1 Personal data shall be processed in accordance with the rights of data subjects.

- 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 not to be subject to automated decision-making including profiling*
- The right to be forgotten

* see key changes in Appendix 1

7. Personal Information covered by this policy

7.1 This policy covers any information that relates to living individuals which is held on computer or in hard copy format. For example, this may include information such as name, address, date of birth and opinions about the individual or any other information from which the individual can be identified.

8. Responsibilities

8.1 All staff, MSAs, volunteers and Trustees are responsible for:

- Ensuring that their processing of personal data, including research data, is compatible with the data protection principles.
- Ensure that paper documents containing personal data are securely stored in lockable cabinets on site and that keys used to lock them are stored securely in the key safe with access granted on a need-to-know basis.
- Where possible, convert paper records to electronic form and restrict access to those that need it.
- Implement a clear desk policy and lock their computer screen when away from their desk.
- Ensure there is no unauthorised access when printing personal details by not leaving the printer unattended - collecting printed material immediately.
- Use strong passwords and ensure they keep the personal data held on their computer secure.
- Ensure access to files that contain personal data is restricted on a need-to-know basis.
- Password-protect files that contain sensitive information in relation to individuals that is not appropriate for all team members to access.
- Ensure the office is kept secure by locking the door wherever it is unattended, for however long this may be.
- Completing relevant Data Protection training made available to them by NWN. This training is provided through our training platform and is part of the staff induction programme.
- Raising any concerns in respect of the processing of personal data in the first instance with the NWN Data Protection lead.
- Passing on all subject access requests and requests from third parties for personal data to the NWN Data Protection lead.
- Reporting unauthorised disclosures of personal data to the NWN Data Protection lead.
- Ensuring that any personal data provided to the organisation is up to date.

8.2 Compliance with these responsibilities should be monitored by Managers in the form of spot checks and results discussed at staff and Board meetings and communication with MSAs and volunteers, particularly where improvements in data protection practice have been identified.

8.3 The NWN Data Protection Lead is the CEO.

8.4 In addition, the Neighbourhood Watch Network Board of Trustees has a data protection lead (Andrew Whyte) who is responsible for ensuring that the Data Protection Lead complies with this policy and the associated sub-policies. Data Protection updates are provided to each Board meeting.

9. Access to Personal Data

9.1 Data subjects have the right to access their personal data held by NWN. The NWN Subject Access Requests Policy outlines staff, MSA, volunteer and Trustee responsibilities in this respect.

9.2 Copies of any information held will be provided to the individual, in their preferred format, normally within a month. *See changes to this in Appendix 1*.

9.3 Neighbourhood Watch Network will not normally charge for any data subject access requests, unless the request is manifestly unfounded or excessive.

10. Monitoring

10.1 It is sometimes necessary for Neighbourhood Watch Network to monitor information and communications. This may include personal data. Neighbourhood Watch Network will endeavour to inform staff members, MSAs and volunteers of the reasons should this happen.

11. Third Party Access

11.1 In certain circumstances Data Protection legislation provides for disclosure of personal data to certain organisations, without the consent of the data subject. Requests for such disclosures from third parties, such as the police, UK Border Agency etc. should be made in writing and will be handled by the Head of Partnerships and Projects.

12. Records Management

12.1 When records are no longer required for operational reasons they must either be transferred to a secure system or disposed of securely and confidentially. All paper documents containing personal details should be shredded. NWN owned computers and laptops should be disposed of by sending them to a suitable contractor who will provide NWN with a certificate of destruction.

For further advice concerning any aspect of this policy please contact the NWN Head of Policy, Partnerships and Projects.

Approved by Trustees March 2026

Appendix 1 - Key changes under DUAA (Data Use and Access)

1. New lawful basis — "Recognised legitimate interests"
    - A seventh lawful basis for processing that does *not* require the usual balancing test for certain public interest purposes (e.g., crime prevention, safeguarding, national security).
2. Automated decision-making (ADM) framework revised
    - The previous broad prohibition on certain automated decisions has been relaxed. Organisations can now use automated systems more broadly if safeguards are in place (e.g., transparency, right to challenge, human review).
3. Children's data protection
    - New obligations for online services likely to be used by children to consider and design protective features.
4. Scientific research and commercial research
    - Clarification that "scientific research" under the law can include commercial studies with appropriate safeguards.
5. International data transfers
    - New criteria for approving transfers — the UK now tests whether a country's standard is "not materially lower" than the UK's (moving away from strict equivalence).
6. Complaints handling
    - Organisations must implement formal complaints processes for concerns about data protection.
7. Storage/access technologies
    - Low-risk cookie storage/access is allowed without explicit consent in certain circumstances (loosening strict consent requirements).
8. Changes to law enforcement & intelligence processing
    - DUAA amends parts of DPA 2018 governing law enforcement and intelligence services to align with new UK GDPR provisions.

Phased commencement

- Many changes began to come into effect in early 2026 (including recognised legitimate interests and lawful basis updates from *5 February 2026*).
- Some requirements (e.g., structured complaints handling) are set to commence mid-2026.

Data (Use and Access) Act factsheets: what has changed

- UK GDPR and DPA factsheet
- PEC Regulations factsheet

- ICO factsheet