Neighbourhood Watch SCOTLAND

Safer Neighbourhoods Stronger Communities

Data Protection Policy

Version Number:	v.1
Written by:	Lynne Symington
Owner:	Board / NWS Director
Approved:	21/04/26 by Chair & Director
Publication Date:	17/05/26
Review Date:	17/05/27

Contents

1. Purpose

NWS is committed to protecting the privacy and personal data of all individuals whose information it holds. This policy sets out how NWS collects, uses, stores, shares, and protects personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 and the rights of individuals whose data is processed.

2. Scope

This policy applies to all personal data stored or processed by NWS during our charitable activities regardless of format or location and includes:

- Neighbourhood Alert (hosted and operated by VISAV Limited)
- The NWS website and online shop
- Email systems
- Shared folders and cloud-based collaboration tools
- Databases and case management systems
- Paper records and physical files

'Personal data' means any information relating to an identified or identifiable living individual and includes data processed via our website, email communications, and the Neighbourhood Alert system.

This policy applies to all employees, trustees, NWS contractors, and volunteers. Volunteers include Neighbourhood Watch coordinators who process personal data on behalf of NWS, including where this data is held in home-based records such as lists or spreadsheets for legitimate Watch purposes.

3. Roles and Responsibilities

3.1 Data Controller

NWS is registered as a Data Controller with the Information Commissioner's Office (ICO) and responsible for ensuring that personal data is collected lawfully; is accurate and secure; and responds to access requests from individuals.

The NWS Director is the Data Protection Lead for NWS.

3.2 Data Protection Officer

The Director as the Data Protection Lead will appoint a Data Protection Officer (DPO) to advise and monitor compliance with data protection laws. The DPO will be responsible for:

- Informing and advising the controller and staff about their obligations under data protection law.
- Monitoring compliance and conduct audits.
- Be the contact point for individuals (data subjects) and the ICO.

3.3. Data Processors

All NWS staff are Data Processors (who act on instructions from the NWS Controller and process personal data on their behalf). They must ensure they

- Follow the controller's instructions exactly (comply with NWS policy and relevant training).
- Keep data secure.
- Assist the controller with GDPR obligations.

3.4 Joint Controller - Neighbourhood Alert System (VISAV Limited)

The Neighbourhood Alert system is a secure partitioned website owned and operated by VISAV Ltd, which enables communication between Police Scotland, Scottish Fire & Rescue, other partner agencies, and registered users. The primary data controller is VISAV Limited. NWS is a joint Data Controller, and its employees access the personal data of registered users as permitted under licence from VISAV. A contractual agreement is in place for this purpose.

4. Principles of Data Protection

This policy follows the requirements of the Data Protection Act 2018 the aim of which is to promote high standards in the handling of personal information and so protect the individual's right to privacy. NWS fully endorses and adheres to the principles of Data Protection, as outlined in the Act which govern that personal data shall be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes, and not further processed in any manner that is incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date.
- Kept in a form which permits identification of data subjects for no longer than is necessary.
- Processed in a manner that ensures appropriate security of the personal data, including protection against accidental or unauthorised access to, or destruction, loss, use, modification, or disclosure of personal data.

5. Lawful Basis for Processing Personal Data

NWS processes personal data under one or more of the following lawful bases:

- **Consent:** when individuals have given clear consent for NWS to process their personal data for a specific purpose (e.g. subscribing to newsletters or joining the Alert system).
- **Legitimate Interests:** for activities that support our charitable aims and community safety objectives, where such interests are not overridden by the rights of individuals.
- **Legal Obligation:** when processing is necessary to comply with legal requirements.

- **Contractual necessity:** where processing is necessary for the performance of a contract or agreement with an individual.
- **Public task**: where processing is necessary to perform a task in the public interest or in the exercise of official authority e.g. Scottish Government.

The lawful basis used depends on the purpose of processing and is documented within internal records of processing activities.

6. Rights of Individuals
All individuals have the following rights:

• The right to be informed – we do this by making sure our privacy notices are accurate.

• To access their personal data (see section 13 below).

• The right to rectification – we will quickly update any personal data which has been identified as inaccurate or incorrect.

• The right to erasure – we will remove any personal data if an individual requests this unless we have another lawful basis which would prevent this e.g. employee records.

• The right to restrict or object – we will cease processing in any dispute about personal data until resolved and will deal with complaints quickly and accurately.

• The right to data portability – we will provide an individual with their data in a common and readable electronic format.

• The right not to be subject to automated decision-making including profiling. NWS does not conduct any automated decision-making or profiling.

7. Type of Data Collected by NWS
This policy covers any information that relates to living individuals which is held on computer or in hard copy format. The information collected depends on the level of interaction e.g. as a website visitor, Alert user, or other means of communications such as email). NWS may collect:

- Name, address, postcode, email, telephone number.
- Organisation or group affiliation (e.g. local Watch group)
- Usernames or login credentials for registered services (managed by VISAV)
- Communication preferences
- Any information such as questions and comments voluntarily submitted via forms, surveys, or correspondence.
- Year of birth (optional when signing up for Alert)

- Ethnicity, gender, religion, disabilities, interest groups, and information provider preferences (optional when signing up for Alert).
- Technical data and information about activities on our website is collected by Google Analytics and Wordfence. These include the time of the visit, pages visited, and time spent on each webpage, referring site details, the type of web browser, type of operating system (OS) Flash version, JavaScript support, screen resolution, network location, and IP address.
- Transaction and order information (online shop) - If placing an order through the NWS website, personal data is collected and stored by WooCommerce and includes email address, home address, name, and phone number. Payment card details are processed securely by third-party payment providers and are not stored by NWS (PayPal).

NWS does not collect special category (sensitive) personal data unless explicitly required and with appropriate safeguards.

8. How NWS Uses Personal Data

NWS uses personal data to:

- Manage and support Neighbourhood Watch groups and members.
- Distribute community safety information and alerts.
- Respond to enquiries and provide support.
- Maintain contact lists for partner and stakeholder engagement.
- Improve our services, websites, and communication methods.
- Meet legal and regulatory obligations.

9. Data Sharing and Third Parties

NWS will only share personal data where necessary and lawful. NWS may share personal data with trusted third parties where necessary, including:

- IT and system providers
- Communication platforms - Neighbourhood Alert data is securely processed and stored by VISAV Ltd, under a Data Processing Agreement. VISAV maintains full compliance with UK GDPR and ISO27001 standards. Neighbourhood Alert data is used solely for its intended purpose and is not sold or used for unrelated marketing. Individuals can unsubscribe or update their preferences at any time.
- Payment processors
- Funders or regulators (where required by law)

- Police and local authority (In certain circumstances Data Protection legislation provides for disclosure of personal data to certain organisations, without the consent of the data subject).

Any such requests for such disclosures from third parties, such as the police, UK Border Agency, should be made in writing and will be managed by the DPO.

All third parties are required to protect personal data appropriately and only process it in accordance with NWS instructions.

NWS does not sell or rent personal data to third parties.

10. Data Security

10.1 NWS Security Measures

NWS takes appropriate technical and organisational measures to protect personal data from unauthorised access, loss, misuse, or disclosure. These measures include:

- Secure, encrypted systems and password protection
- Restricted access to personal data based on role.
- Staff and volunteer awareness training
- Secure transfer and storage of electronic and paper records. Digital information is stored in a secure online environment, which has been awarded Cyber Essentials accreditation. It is accessible only by employees of NWS and by system administrators representing the approved Information Providers. Full Terms and Conditions are available at the point of registration.

10.2 NWS Shared Folders and Internal Systems

Personal data may be stored within shared folders and internal systems used by NWS staff and trustees. NWS ensures that:

- Access to shared folders is restricted on a need-to-know basis.
- Only approved systems and platforms are used.
- Personal data is not stored in personal cloud accounts or unauthorised locations.
- Unnecessary duplication of personal data is avoided.

All personal data stored in shared folders is subject to the same security and retention requirements as data held elsewhere.

10.3 General Responsibilities of staff, trustees, and volunteers

All employees, trustees and volunteers are therefore responsible for:

- Ensuring that any personal data provided to the organisation is up to date.
- Ensuring that their processing of personal data, including research data, is compatible with the data protection principles.
- Ensuring that paper documents containing personal data are securely stored.

- Where possible, paper records are to be converted to electronic form and access restricted to those that need it.
- Adhering to a clear desk policy and lock their computer screen when away from their desk.
- Ensuring there is no unauthorised access when printing personal details.
- Using strong passwords and ensuring they keep the personal data held on their computer secure.
- Ensuring access to files that contain personal data is restricted.
- Password protecting files that contain sensitive information in relation to individuals that is not appropriate for all team members to access.
- Raising any concerns in respect of the processing of personal data in the first instance with the Director or DPO.
- Passing on all subject access requests and requests from third parties for personal data to the Director or DPO.
- Reporting unauthorised disclosures of personal data to the Director or DPO.

10.4 Neighbourhood Watch Coordinators and Home-Based Records

Neighbourhood Watch coordinators may, as part of their role, maintain limited personal data relating to Watch members (such as names and contact details) for communication and circulation purposes.

Such data is processed on behalf of NWS, which remains the data controller.

Coordinators must:

- Only hold the minimum personal data necessary.
- Use the data solely for Watch-related purposes.
- Keep data secure, including when stored at home.
- Avoid sharing data without authorisation and consent.
- Delete or securely dispose of data when it is no longer required or when they step down from the role.

11. Data Retention and Records Management

NWS retains personal data only for as long as necessary to fulfil the purpose for which it was collected and to meet legal, regulatory, or contractual requirements. Retention periods are set out in the NWS Data Retention Schedule, which forms part of this policy (Appendix A).

When data is no longer required, it must be securely deleted, destroyed, or anonymised.

When paper 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.

NWS owned computers and laptops should be disposed of by sending them to a suitable contractor (Black Frog) who will provide NWS with confirmation of destruction.

12. Data Breach Procedure

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All trustees, employees and volunteers must be able to identify a suspected personal data breach. A breach could include:

- Access by an unauthorised third party to personal data
- Deliberate or accidental action (or inaction)
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen.
- Alteration of personal data without permission
- Loss of availability of personal data
- Leaving a file on a train.

Where a member of staff discovers or suspects a personal data breach, this should be reported to the DPO / Director or Chair as soon as possible. NWS will immediately investigate the breach and take steps to minimise harm.

Where there is a likely risk to individuals' rights and freedoms, the DPO will report the personal data breach to the **ICO within 72 hours** of NWS being aware of the breach.

Further, where there is a likely risk to individuals' rights and freedoms, NWS will inform those individuals without undue delay.

The DPO will keep a record of all personal data breaches reported and follow up with appropriate measures and improvements to reduce the risk of occurrence. And improve future resilience.

13. Individuals Rights: Access to Information

Under UK GDPR, individuals have the right to:

- Be informed about how their data is used.
- Access their personal data.
- Request correction of inaccurate data.
- Request deletion of data (where applicable)
- Restrict or object to processing.
- Data portability
- Withdraw consent.

All requests should be submitted to the DPO and copies of any information held will be provided to the individual, in their preferred format, within a month. NWS will not charge for any data subject access requests unless the request is manifestly unfounded or excessive.

Data subjects should direct any queries or requests to exercise data rights, to the:

Data Protection Officer (DPO)
Neighbourhood Watch Scotland
Registered Office: 21 Claylands Road, Newbridge, Edinburgh, EH28 8LF
Email: Info@neighbourhoodwatchscotland.co.uk
Phone: 01786 463732 (main office)
Website: https://www.neighbourhoodwatchscotland.co.uk

Anyone who is dissatisfied with the NWS response, has the right to complain to the UK Information Commissioner's Office (ICO): **https://ico.org.uk/concerns**

14. Conclusion

It is the responsibility of all staff, trustees, and volunteers of NWS to ensure that they manage personal data in accordance with this policy, complete any required training and report any data protection concerns promptly. Failure to comply may result in disciplinary action.

To ease understanding and aid easy reference the following appendices have been included:

- Appendix B: Neighbourhood Alert (Processing Overview)
- Appendix C: Website & Online Shop (Processing Overview)
- Appendix D: Data Handling Guidance (Easy Reference)
- Appendix E: NWS - Data Protection Guidance for Watch Coordinators

15. Review Arrangements

This policy will be reviewed annually or sooner if there are changes to legislation, guidance, or NWS activities.

Furthermore, to ensure the processing of data is lawful, fair, and transparent, NWS shall keep and maintain Data Audits to record where and why we process personal data. The Data Audits will be kept up to date and reviewed annually.

Appendix A: NWS Data Retention Schedule

This retention schedule applies to all personal data processed by NWS, regardless of format or storage location, including shared folders, cloud systems, email, databases, and paper records.

1. Governance, Staff & Volunteers

Data Category	Examples	Purpose	Lawful Basis	Retention Period	Disposal
Staff records	Contracts, HR files	Employment management	Contract / Legal obligation	6 years after employment ends	Secure deletion / shredding
Volunteer records	Contact details, role info	Volunteer management	Legitimate interests	2 years after role ends	Secure deletion
Trustee records	Appointment details	Governance	Legal obligation	6 years after role ends	Secure deletion
Training records	Completion logs	Compliance & assurance	Legitimate interests	3 years after training	Secure deletion

2. Neighbourhood Alert (hosted by VISAV Limited)

This platform is hosted by VISAV. Please refer to the VISAV terms and conditions for system management and retention schedule (Third-party providers must meet UK GDPR requirements).

Data Category	Examples	Purpose	Lawful Basis	Retention Period	Disposal
Subscriber details	Name, email, location	Sending alerts & updates	Consent / Legitimate interests	Until user unsubscribes	Automated deletion
Communication preferences	Opt-ins, opt-outs	Compliance	Legal obligation	Until withdrawn	Automated deletion
Alert logs	Message history	Audit & assurance	Legitimate interests	24 months	Secure deletion

Notes: Individuals can unsubscribe at any time.

3. Website & Online Shop

Website

Data Category	Examples	Purpose	Lawful Basis	Retention Period	Disposal
Contact form enquiries	Name, email, message	Responding to enquiries	Legitimate interests	12 months	Secure deletion
Website analytics	IP address (anonymised)	Site improvement	Legitimate interests	14 months	Automated deletion

Online Shop

Data Category	Examples	Purpose	Lawful Basis	Retention Period	Disposal
Order records	Name, address, order details	Fulfilment & accounting	Contract / Legal obligation	6 years	Secure deletion
Payment references	Transaction IDs	Audit & reconciliation	Legal obligation	6 years	Secure deletion

Note: NWS does not store payment card details. These are managed securely by third-party payment providers.

4. Communications & Engagement

Data Category	Examples	Purpose	Lawful Basis	Retention Period	Disposal
Email correspondence	Queries, responses	Ongoing engagement	Legitimate interests	2 years after last contact	Secure deletion
Event registrations	Attendance lists	Event management	Legitimate interests	12 months	Secure deletion
Feedback & surveys	Responses	Service improvement	Legitimate interests	24 months	Anonymisation

5. Shared Folders & Internal Documents

Data Category	Examples	Purpose	Lawful Basis	Retention Period	Disposal
Operational documents	Reports with personal data	Service delivery	Legitimate interests	In line with relevant category	Secure deletion
Working drafts	Draft documents	Operational use	Legitimate interests	Deleted when no longer needed	Secure deletion
Duplicate files	Copies in shared folders	Convenience	Legitimate interests	Avoided / deleted promptly	Secure deletion

Key rule: Personal data stored in shared folders must not be retained beyond the approved retention period for that data type.

6. Safeguards & Review

- Retention periods are reviewed annually.
- Data owners are responsible for ensuring compliance.
- Secure deletion methods are used for all disposals.
- Retention applies regardless of storage location.

Appendix B: Neighbourhood Alert (Processing Overview)

1. Purpose of Neighbourhood Alert

Neighbourhood Alert is used by Neighbourhood Watch Scotland (NWS) to provide timely information and updates relating to community safety, crime prevention, and related matters. The system supports NWS's charitable objectives by enabling effective communication with individuals who have chosen to receive alerts.

The Neighbourhood Alert system is a secure partitioned website owned and operated by VISAV Ltd, which enables communication between Police Scotland, Scottish Fire & Rescue, other partner agencies, and registered users. The primary data controller is VISAV Limited. NWS is a joint Data Controller, and its employees access the personal data of registered users as permitted under licence from VISAV. A contractual agreement is in place for this purpose.

2. Categories of Personal Data

NWS may process the following personal data through Neighbourhood Alert:

- Name
- Email address and telephone number.
- Location (home address) or geographical area of interest
- Communication preferences
- Subscription and unsubscribe records.

No special category personal data is intentionally collected through Neighbourhood Alert.

3. Purpose of Processing

Personal data within Neighbourhood Alert is processed for the following purposes:

- Sending community safety alerts and updates
- Sharing crime prevention advice and relevant information
- Managing subscriptions and communication preferences
- Demonstrating compliance with data protection requirements

4. Lawful Basis for Processing

The lawful basis for processing Neighbourhood Alert data is:

- Consent, where individuals actively sign up to receive alerts.
- Legitimate interests, where communication is necessary to support NWS's charitable aims and individuals would reasonably expect to receive such communications.

Individuals can withdraw consent or object to processing at any time.

5. Data Sharing and Processors

The Neighbourhood Alert system is a secure partitioned website owned and operated by VISAV Ltd, which enables communication between Police Scotland, Scottish Fire & Rescue, other partner agencies, and registered users. The primary data controller is VISAV Limited. NWS is a joint Data Controller, and its employees access the personal data of registered users as permitted under licence from VISAV. A contractual agreement is in place for this purpose; data is only processed in accordance with NWS instructions and is not sold or shared for unrelated purposes.

6. Retention

Neighbourhood Alert data is retained only for as long as individuals remain subscribed or as required for audit and compliance purposes.

Retention periods are set out in the NWS Data Retention Schedule (Appendix A) and in the VISAV terms and conditions.

7. Individual Rights

Individuals using Neighbourhood Alert have the right to:

- Access their personal data.
- Update or correct their details.
- Unsubscribe from communications.
- Object to processing

Requests are managed in line with UK GDPR requirements.

8. Security Measures

NWS takes reasonable technical and organisational measures to protect Neighbourhood Alert data, including:

- Restricted system access
- Password protection
- Supplier due diligence

Appendix C: Website & Online Shop (Processing Overview)

1. Website Processing

1.1 Personal Data Collected

The NWS website may collect personal data through:

- Contact forms.
- Event or engagement enquiries (including by phone)
- Cookies and analytics tools

1.2 Purpose of Processing

Website data is processed to:

- Respond to enquiries.
- Provide requested information.
- Improve website performance and usability.
- Maintain website security.

1.3 Lawful Basis

The lawful basis for website processing includes:

- Legitimate interests, to respond to enquiries and improve services.
- Consent, where individuals sign up to receive communications or accept non-essential cookies.

2. Online Shop Processing

2.1 Personal Data Collected

When individuals make a purchase through the NWS online shop, NWS may collect:

- Name
- Contact details.
- Delivery address
- Order details

Payment card information is processed securely by third-party payment providers and is not stored by NWS.

2.2 Purpose of Processing

Online shop data is processed for:

- Order fulfilment
- Customer communication
- Financial record-keeping and audit

2.3 Lawful Basis

The lawful basis for online shop processing is:

- Contract, to fulfil orders.
- Legal obligation, for accounting and financial records

3. Data Sharing

Personal data collected through the website and online shop may be shared with:

- Website hosting providers
- Payment processors
- Delivery partners
- IT service providers

All third parties are required to manage data securely and lawfully.

4. Retention

Website and online shop data is retained only for as long as necessary.

Retention periods are detailed in the NWS Data Retention Schedule (Appendix A).

5. Security

NWS applies appropriate safeguards, including:

- Secure hosting environments
- Access controls
- Regular system updates

Appendix D: Data Handling Guidance (Easy Reference)

This guidance applies to all staff, volunteers, trustees, and contractors working with Neighbourhood Watch Scotland (NWS).

Your Responsibilities

If you manage personal data as part of your role, you must:

- Use personal data only for NWS business.
- Follow NWS policies and guidance.
- Keep data accurate and up to date.
- Report concerns or incidents immediately.

What Counts as Personal Data?

Personal data includes names and contact details; email addresses; home addresses and location information, and any information that can identify a living person.

Using Personal Data Safely

You must:

- Only access data you need for your role
- Use NWS-approved systems and shared folders.
- Keep passwords secure.
- Lock screens and files when not in use.

You must not:

- Store NWS data in personal email or cloud accounts.
- Download data unless necessary.
- Keep data “just in case.”

Home Use of Personal Data (Watch Coordinators)

If you are a Watch Coordinator and keep member details at home:

- Use password-protected devices where possible.
- Do not store data on shared family computers without protection.
- Avoid printing unless necessary.
- Do not keep old or unused lists.
- Transfer data securely if passing the role to another Coordinator.
- Delete when no longer required or at request by member.

NWS Shared Folders

When using shared folders:

- Avoid unnecessary duplication.
- Save files in the correct location.
- Delete personal data when it is no longer needed.
- Comply with retention schedule (Appendix A)

Emails & Communications

- Double-check recipients before sending emails.
- Use BCC where appropriate and do not share personal data unless authorised.

Data Breaches

A data breach includes sending data to the wrong person, losing a device or paper file and any unauthorised access to data.

Report any suspected breach immediately. Early reporting helps protect individuals and NWS.

Individual Rights

People have the right to see their data; correct errors and ask for deletion in some cases. If you receive a data request, pass it to the DPO or Director promptly.

Remember: If you are unsure — ask before acting.
Protecting personal data is everyone's responsibility.

Appendix E: NWS - Data Protection Guidance for Watch Coordinators

This guidance applies to all local Neighbourhood Watch coordinators who keep or use member contact details as part of their role. As a Watch Coordinator, you may keep a list of Watch members to help with communication and circulation of information. These details are **personal data**, and Neighbourhood Watch Scotland (NWS) has a legal duty to make sure they are managed safely. This guidance explains what is expected of you and helps protect both you and your Watch members.

What personal data you may hold

You may hold only what is necessary, such as:

- Names
- Addresses
- Email addresses
- Phone numbers

You should not collect or keep extra information unless there is a clear Watch-related reason.

How you can use this information

You may use member details only for Neighbourhood Watch-related communication, circulating crime prevention or community safety information and organising Watch activity.

You must not use the information for personal reasons, share it outside the Watch without permission or use it for marketing or non-Watch activities.

Storing information at home

If you keep member details at home (for example in a spreadsheet or notebook):

Do

- Keep digital files on a password-protected device.
- Lock paper records away when not in use.
- Keep information up to date.
- Delete or securely dispose of old or unused lists.
- Delete data at the request of a member.

Do not!

- Store Watch data on shared family computers without protection.
- Keep multiple unnecessary copies.
- Leave papers where others can see them.

- Upload data to personal cloud accounts.
- Print unless necessary.
- Keep old or unused lists.

Emails and circulation

When sending emails:

- Double-check email addresses before sending.
- Use BCC when emailing multiple members.
- Keep messages Watch-related and relevant.

When you step down or hand over

If you stop being a Coordinator:

- Pass on any necessary information securely to the new Coordinator.
- Delete or securely destroy all Watch member data (e.g. shred paper copies).
- Do not keep copies "just in case."

Data breaches – what to do

A data breach could include sending an email to the wrong person; losing a device or paper list; or someone accessing data without permission. If this happens: Report, any data breach to NWS as soon as possible!

Early reporting helps reduce risk and protects everyone.

Your role and NWS's role

- NWS is the data controller.
- You, as a formal Watch Coordinator, are authorised to use data as part of your Coordinator role.
- If you adhere to this guidance and report issues promptly you will reduce the risk of personal liability.

Questions or concerns?

If you are unsure about anything: Ask before acting…

Contact the NWS Data Protection Officer (DPO) at:

Neighbourhood Watch Scotland
21 Claylands Road, Newbridge, Edinburgh, EH28 8LF
Email: Info@neighbourhoodwatchscotland.co.uk
Phone: 01786 463732 (main office)
Website: https://www.neighbourhoodwatchscotland.co.uk.

Protecting personal data is part of keeping our communities safe — thank you for helping us do it properly.