



NEIGHBOURHOOD WATCH NETWORK

SUBJECT ACCESS REQUEST

POLICY AND PROCEDURES

Author: Sandra Bauer
Approved: 09 November 2022
Next review due: 07 November 2024

1. Introduction

- 1.1 Data Protection legislation including GDPR entitles data subjects to have access to personal information that is held about them. This policy details the issues that need to be taken into consideration when responding to a Subject Access Request (SAR) and outlines the process and NWN staff responsibilities.
- 1.2 The Freedom of Information Act 2000 provides public access to information held by public authorities. As NWN is a Charitable Incorporated Organisation (CIO) and not a public authority it is therefore not bound by the requirements of the Freedom of Information Act 2000.

2. What information is an individual entitled to?

- 2.1 Individuals have the right to obtain the following:
- confirmation that NWN is processing their personal data;
 - a copy of their personal data; and
 - other supplementary information – this largely corresponds to the information that NWN provides in a privacy notice (see ‘Supplementary information’ below).

3. Individuals entitled to receive copies of personal records held by Neighbourhood Watch Network

- 3.1 An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone e.g. those with parental responsibility (parent/legal guardian).
- 3.2 Personal information must not be disclosed to a third party unless and until authorisation is obtained from the individual data subject.

4. ‘Supplementary information’

- 4.1 In addition to a copy of their personal data, NWN also has to provide individuals with the following information:
- the purposes of our processing;

- the categories of personal data concerned;
- the recipients or categories of recipient NWN discloses the personal data to;
- NWN's retention period for storing the personal data or, where this is not possible, the criteria for determining how long NWN will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, if it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- safeguards NWN provides if NWN transfers personal data to a third country or international organisation.

4.2 NWN provides much of this information already in our **Privacy Notice**. A copy of this privacy notice should accompany any personal data sent to the individual.

5. Receiving a request for personal information

5.1 A request for access to an individual's personal information held by Neighbourhood Watch Network can be made either in writing (by letter or e-mail) or verbally. It can also be made via social media and does not have to be made to a specific person or contact point within NWN.

5.2 Identity of the requester. If we are not sure the requester is who they say they are, we must check this quickly. We shouldn't ask for formal ID unless it's necessary and proportionate. Instead, we can ask questions that only they would know about reference numbers or equivalent. Or we can ask for ID that we can verify. There's little point insisting on photo ID if we don't know what the requester looks like – it should be proportionate.

5.3 A request does not have to include the phrase 'subject access request' or Article 15 of the GDPR, as long as it is clear that the individual is asking for their own personal data.

5.4 If the Subject Access Request is made verbally the staff member receiving it will record and date it in the Subject Access Requests log in the Admin folder on the NWN shared drive. The received date should be recorded on all written requests for records and these should similarly be recorded on the Subject Access Requests log. All Subject Access Requests received by staff should be notified to the NWN administrator who will process the request in liaison with the NWN Data Protection lead.

5.5 The Subject Access Request application must contain sufficient information to enable NWN to locate the information requested. The receiving staff member will check that the application fulfils the following criteria:

- Full name, e-mail address, home address (if relevant) of applicant is provided.
- Identification documentation has been provided where necessary.
- The Subject Access Request is dated by the receiving staff member.
- If someone else is acting on behalf of the applicant appropriate authorisation is given by the data subject.
- The Subject Access Request provides enough data to identify where the records are being held.

- 5.6 If the application is deemed to be incomplete, the NWN Administrator will log details of request and then send either an e-mail or a letter or contact the person via social media (dependent upon the original channel the SAR was made through) requesting the necessary information to complete the application. The deadline of one month for a response to the SAR will start from the date of receipt of the completed application.
- 5.7 If, after 3 months, no reply with further information has been received from the person requesting the data, the request will be destroyed using confidential means.
- 5.8 Data Protection legislation imposes a 1 month limit on disclosing personal records in response to a SAR unless it is complex / numerous. To ensure NWN complies with this time limit, a deadline of 28 days will apply from the date of receipt of a completed request to disclosing the requested information. If the request is complex or there are numerous requests from the same individual then this limit can be extended by up to a further 2 months. The data subject must be notified of any extension and the reason for it within 28 days of receipt of the original request.

6. Acknowledging a request for personal information

- 6.1 Once a Subject Access Request has been received by NWN, the request will be logged in the Subject Access Request register by the staff member receiving the request within 24 hrs of receipt. An acknowledgement will be sent by the NWN Administrator to the applicant stating that Neighbourhood Watch Network is currently processing their request. This acknowledgement will be sent by e-mail, letter or via social media (dependent upon the original channel the Subject Access Request was made through).

7. Processing the Subject Access Request

- 7.1 When a Subject Access Request is received by NWN then the following systems need to be checked for any personal data held on the Data Subject making the request: -
- All Staff members' e-mails
 - Saved documents or e-mails on all staff member's work pc or laptops
 - The NWN Shared Drive on Microsoft 365
 - Any USB sticks used by staff
 - Hard copies of membership information / job applications / tenders for contracts etc. held in the NWN Office or at staff home addresses
 - The OurWatch website
 - All correspondence records received by NWN
 - The Neighbourhood Watch Register

8. Data held by another organisation / party

- 8.1 If the request indicates that data may be held by the local NW either at Force Area Association or Coordinator level, the NWN administrator will advise the requester that they may also wish to submit a Subject Access Request to their Force Area NW Association as obligations under the Act are in general placed on the holder of the record.
- 8.2 Where there is no association in place and information relevant to the SAR may be held locally, then the requester may be advised to submit a Subject Access Request to their local Police force for checks of any records they keep about Neighbourhood Watch membership.

- 8.3 If records are shared between two parties as joint data controllers, each organisation /party is obliged to deal with the access request and the authorisation to release the parts of the record they hold in order to ensure the request is processed within the one month timescale. Each organisation / party processing the access request will accept full responsibility for their own decisions with regard to that request.
- 8.4 If personal data about the Data Subject is contained within the Neighbourhood Watch Scheme Register or otherwise on the Neighbourhood Alert system, the Subject Access Request will also be forwarded to VISAV, that own the Neighbourhood Alert system, for them to provide the personal data held on that system in an accessible format. In these circumstances, it will be agreed between NWN and VISAV who will respond to the Subject Access Request, dependent upon which organisation is the data controller, or, where the data is jointly controlled, whether other personal data is held about the data subject by either organisation.

9. Fees

- 9.1 In most cases a fee cannot be charged to comply with a subject access request.
- 9.2 However, where the request is manifestly unfounded or excessive a “reasonable fee” may be charged for the administrative costs of complying with the request.
- 9.3 A reasonable fee can also be charged if an individual requests further copies of their data following a request. The fee must be based on the administrative costs of providing further copies.
- 9.4 If a request is manifestly unfounded or excessive NWN can refuse the request. In any such cases NWN will seek advice from the ICO.

10. Reviewing the personal records

- 10.1 It is the responsibility of the NWN Data Protection lead to review the record prior to its release and to decide what information, if any, should be released and what should be withheld. This review will verify:

- a. If there are any references to third parties.

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual. NWN does not have to comply with the request if to do so would mean disclosing information about another individual who can be identified from that information, except where:

- the other individual has consented to the disclosure; or
- it is reasonable in all the circumstances to comply with the request without that individual’s consent.

Although NWN may sometimes be able to disclose information relating to a third party, a decision needs to be taken whether it is appropriate to do so in each case. This decision will involve balancing the data subject’s right of access against the other individual’s rights in respect of their own personal data. If the other person consents to NWN disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, NWN must decide whether to disclose the information anyway.

- b. If there are any abbreviations or complex terms which require explanations as to the content or their meaning (for example use of codes, jargon or acronyms) NWN can offer to 'go through' the information with the data subject to explain the meanings.
- c. If there are grounds to withhold information under other exemptions in the data protection legislation / GDPR, a record must be made in the Subject Access Request register of information withheld, along with justification of the exemptions that were applied. These grounds should be notified to the requester in the response letter.

11. Finalising the request

- 11.1 The NWN administrator will send an e-mail or letter to the requester to accompany the information intended for release. This should confirm the response to the original request.
- 11.2 Records will not be forwarded on to third parties but will only be sent to the original applicant.
- 11.3 If an individual makes a request electronically, the information should be provided in a commonly used electronic format, unless the individual requests otherwise.
- 11.4 Copies of records sent externally in the post should be:
 - In a sealed, tamper-proof envelope e.g. self-sealing jiffy bag
 - Addressed to a named person
 - Marked 'Private and Confidential'
 - Sent by special/recorded delivery
- 11.5 The NWN administrator will ensure that the Subject Access Request register contains a record of the date the final correspondence was sent and then mark the request in the register as "closed". A record of what was sent out in response will be kept either in hard copy in a locked drawer and marked "subject copy" or in the Data Subject Copies SARS folder. All correspondence must be kept on file for two years, in case any further action is required.
- 11.6 If the data subject themselves indicates that information about him or her is inaccurate or claims that the processing causes them damage or distress, the NWN Data Protection lead will investigate to review the information provided and respond to the data subject outlining the result of their review. If requesters are not satisfied with the response they should be informed of their right to complain to the ICO.

12. Summary of Responsibilities

- 12.1 Staff members will:
 - Log any Subject Access Requests they receive in the Subject Access Request register.
 - Record the date the request is received on any hard copy of the request and in the Subject Access Request register.
 - Ensure the NWN administrator is aware that the request has been received and receives a copy of the request.
 - Check their own desktop, laptop, USB stick(s) and hard copy data for any reference to the data subject.
 - Provide any data relating to the Data Subject to the NWN Administrator

12.2 The NWN Administrator will:

- Ensure details of the request have been entered into the Subject Access Request register.
- Ensure the date the application was received is recorded.
- Ensure that the request contains sufficient detail for it to be processed.
- Send an acknowledgement of receipt of the application to the requester (requesting further information if necessary).
- Where relevant, record the date the request for information was sent to the appropriate staff member or Visav / other organisations with shared data and to whom it was sent.
- If appropriate, start to process the request themselves
- Record the date information was returned from appropriate staff member or Visav.
- Send the requester the information released accompanied by a letter confirming the response to the original request.
- Retain a copy of the data sent to the requester marked 'subject copy' in hard copy in the locked drawer or in the Data Subject Copies SARs folder in SharePoint.
- Mark the request closed in the register.

12.3 The NWN Data Protection Lead is responsible for:

- Ensuring consent is obtained from the individual for the release of their records in accordance with the requirements of the data protection legislation including GDPR.
- Liaising with Visav or other organisations to process the Subject Access Request in the event of shared records/data.
- Co-ordinating the release of the information and ensure that sufficient identification is given by the applicant where necessary.
- Ensuring NWN has a system in place to respond to requests with a responsible individual identified to assist or manage the process.
- Ensuring requests are responded to promptly within the agreed timescales,
- Ensuring the record / data is reviewed before it is sent to the data subject.
- Where a specific request for components of a record or specific information is received, to identify and approve these components for release.
- Investigate in circumstances where the data subject claims the information held by NWN is incorrect or the processing causes them damage or distress.
- Informing the data subject of their right to complain to the ICO
- Ensuring relevant staff are aware of NWN procedures for Subject Access Requests under the data protection legislation including GDPR.

12.4 Advice on data protection / confidentiality is available from the NWN Data Protection lead or www.ico.gov.uk.