NEIGHBOURHOOD WATCH NETWORK

DATA BREACH POLICY AND PROCEDURE

Reviewer: **Sandra Bauer**

Approved: **09 November 2022**

Next review due: **08 October 2024**

1. Introduction

1.1 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. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than simply about losing personal data.

2. Scope

2.1 This policy applies to all Neighbourhood Watch Network staff, Multi Scheme Administrators (MSAs), other Neighbourhood Watch members that process Neighbourhood Watch data and Trustees.

3. Assessing the Risk of a Data Breach

3.1 If NWN experiences a breach of personal data controlled by NWN, whether held on the Neighbourhood Watch Register on the Alert system or otherwise, this should be immediately reported by the staff member, MSA, NW member or Trustee initially becoming aware of the breach to the Head of Partnerships and Projects, the CEO or another available NWN manager. They will consider the likelihood and if so, the severity, of any risk to people's rights and freedoms, following the breach. When this assessment has been made, if it is likely there will be a risk then the ICO must be notified; if this is unlikely, then the breach doesn't have to be reported. Not every breach needs to be reported to the ICO. A self-assessment tool is available to help you decide.

3.2 If NWN becomes aware of a data breach of personal data held on the Neighbourhood Alert system that is controlled by VISAV Ltd, not NWN, then the staff member, MSA or Trustee becoming aware of the breach must ensure that VISAV are informed immediately.

3.3 All decisions about reporting or not reporting data breaches to the ICO must be recorded in the Data Breach Notification Log (See 6.1 below). Whether or not the breach is serious, a log of all activities and steps taken in the time after the breach was discovered must be made. Keeping a detailed record of events will be important in terms of learning lessons and ensuring that everything necessary has been done.

4. Reporting a Data Breach

4.1 If it is decided that the breach needs to be reported to the ICO, NWN must notify them within 72 hours of becoming aware of the essential facts of the breach.

4.2 The breach will generally be reported by telephone to the ICO helpline on 0303 123 1113. Normal opening hours are Monday to Friday between 9am and 5pm. They will record the breach and give advice about what to do next. Reporting a breach outside of these hours can be done online (See below).

4.3 The person making the report will ensure they have the below information or as much of it as is available to hand: -

- name and contact details of the staff member the ICO should liaise with
- what has happened
- when and how the breach was discovered
- basic information about the type of breach
- basic information about the personal data concerned
- the people that have been or may be affected by the breach
- what steps NWN is taking following the breach
- who the ICO should contact if they need more information
- who else has been told.

4.4 If possible, full details of the incident should be included, together with the number of individuals affected and its possible effect on them, the measures taken to mitigate those effects, and information about any notification made to those people affected.

4.5 If these details are not yet available, the incomplete report should be submitted to: - https://report.ico.org.uk/security-breach/ and further details provided to the ICO as soon as possible.

4.6 A second notification report must be submitted to the ICO within 72 hours, either including these details, or telling them how long it will take to get them.

4.7 If NWN experiences a data breach that needs to be reported to the ICO and the CEO is confident it has been dealt with appropriately, it can be reported online. An online report can also be made if the breach is still under investigation and more information will be provided at a later date (within the period above). The online form can also be used to report breaches outside normal ICO opening hours.

https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc

5. Notifying Users Affected by a Data Breach

5.1 If the breach is likely to adversely affect the personal data or privacy of users, users affected need to be notified of the breach without unnecessary delay. They need to be told: -

- The name and contact details of the NWN contact;
- the estimated date of the breach;
- a summary of the incident;
- the nature and content of the personal data;
- the likely effect on the individual;

- any measures NWN has taken to address the breach; and
- how they can mitigate any possible adverse impact.

5.2 Users do not need to be told about a breach if NWN can demonstrate that the data was encrypted (or made unintelligible by a similar security measure).

5.3 If users are not told, the ICO can require NWN to do so if they consider the breach is likely to adversely affect them.

6. Keeping Records

6.1 NWN must also keep a record of all personal data breaches in an inventory or log. Documents can be attached if necessary. The Data Breach Notification Log can be found in the Data Protection Policies and Forms section in the Admin folder on the Shared drive and must contain:

- the facts surrounding the breach;
- the effects of the breach; and
- remedial action taken.

6.2 The Data Breach Notification Log should be submitted to the ICO should a breach need to be reported to them.

6.3 Understanding and assessing the risk in personal data breaches is helpful information to guide a response to this kind of event.