Neighbourhood Watch
Multi Scheme Administrator
Information Pack

1. What is a Multi Scheme Administrator (MSA)?

1.1 An MSA is an Administrator who is granted access to personal data of users and a set of Neighbourhood Watch scheme management tools on the Neighbourhood Alert system in order to manage more than one NW scheme.

1.2 An MSA can be authorised by their local Neighbourhood Watch Force Area / Borough Association lead (or by NWN in the absence of an area /Borough lead) to access user data on the Neighbourhood Alert system for any geographical area that the Association lead defines. This could be an area of a few miles or the entire Force Area or Borough.

1.3 MSAs update and process the personal data of the Neighbourhood Alert users they have access to on behalf of Neighbourhood Watch Network and Visav. This document outlines limitations and rules about how this data can be used by MSAs. Any use of the data outside of these guidelines must have prior approval from either NWN or Visav.

1.4 MSAs can add and delete users, update user contact details, add NW schemes, introduce newly registered users to NW schemes, produce reports, manage NW scheme maps and see an overview of their entire authorised area.

1.5 Importantly, an MSA is able to access the personal data of users that have registered on any Neighbourhood Alert system - as long as that user has agreed (and continues to agree) that 'Neighbourhood Watch' can see their details. This means that MSAs can see individuals who are registered on the Alert system but are not associated with a NW scheme as well as NW scheme coordinators, NW scheme deputies and NW scheme members.

1.6 This access to personal data means that the MSA role is one of great responsibility and must not be entered into lightly. The role you have in managing the information held on the Alert system and correcting out-of-date data will directly assist the police and NW to deliver important messages to people effectively. It will also enable you to reach out to new potential NW members far more easily than ever before.

1.7 It is important therefore, that MSAs act within the parameters set out in this information pack and use the personal data held on the Alert system only for the reasons set out at section 4 below. If an MSA has ideas about how data held on the system could be used to improve scheme management and better support them in their role, advice should be sought from NWN CST before any data is used, to ensure its use complies with Data Protection legislation and is authorised by NWN as data controllers.

2. How much time will it take?

2.1 The role is voluntary and you can give as much time as you feel able to, based on your circumstances. Some MSAs manage ten minutes most weeks, others have been known to work on the system for up to 40 hours a week.

3. What training and support will I receive?

3.1 You will receive training and support in order to perform the role effectively. This will be provided locally from an experienced MSA or by NWN. Where it is necessary for you to travel to attend training provided by NWN, travel expenses will be provided.

3.2 Support is available from the NWN Central Support Team for operational issues enquiries@ourwatch.org.uk and technical support from the Visav Support Desk support@neighbourhoodalert.co.uk or on 0115 9245517. NWN CST can also put you in contact with other experienced MSAs across England and Wales for further practical support.

4. What are the general tasks performed by an MSA?

4.1 Correct Communications Issues

4.1.1. Every user at some time or another will change some element of their data: their email address; phone number(s) or postal address. Unfortunately, members also die, but their account remains on the system and emails and phone calls have been known on other systems to be sent to the surviving spouse for years to come.

4.1.2. One of the most valuable and beneficial tasks that hundreds of trained MSAs perform is in updating the contact information of registered users to whom messages are not getting through. The Alert system will automatically read the replies it receives back from dead or full email addresses and monitor phone numbers to ensure that they are still active. If a problem is detected, the system places the user's account in a 'Communications Issues' list for inspection by a Multi Scheme Administrator.

4.1.3 A few minutes a day, or week spent investigating these issues for users in your local area will assist in maintaining an accurate, efficient contact list which can then be used by Neighbourhood Watch and other Information Providers on the system, such as the police, to ensure that messages are being delivered successfully.

4.2 Identify NW schemes within their area that have not been mapped

Contacting the coordinator of schemes determined as being 'within their area' by the address given by the registered coordinator to get these schemes correctly mapped.

4.3 Identify schemes without a coordinator

Contacting a NW member to identify their local NW scheme coordinator and link the user up with the scheme.

4.4 Approve schemes within their area

Using their own local criteria to determine whether schemes are approved or not. This could involve contacting coordinators to make sure they have undergone whatever local procedure is

necessary in the MSA's area to be recognised as an 'official' scheme (for example registering with the police or contacting their local NW Association).

4.5 Send messages within their area

4.5.1 These could be any messages relevant to NW members and coordinators in an MSA's area, subject to any restrictions and advice from their local police force (see Annex C for general restrictions and advice).

4.5.2 An MSA has the ability to target messages to smaller geographical areas (e.g. a certain radius of a town or village) and can also send messages to specific groups of individuals, for example: certain age groups; nationalities; ethnic groups or interest groups; or only to approved users.

4.6 Deal with user queries

4.6.1 Users might contact an MSA for help with editing their details on the system or sending a login reminder.

4.6.2 If an MSA can't help them or answer their question, they can take their query to a more experienced MSA or an Area or District Administrator (depending on the structure in an area) or seek support from the Visav Support line.

5. How to apply for a role as an MSA

5.1 The MSA role is entirely voluntary. Your application requires approval by your Force Area or Borough NW lead (or by NWN in the absence of an area /Borough lead) and may also require some form of approval by your local police force dependent upon local agreements. No payment is charged or made for time you contribute.

5.2 If you are interested in this role please read and review the **Administration Access Agreement, Rules & Conventions, Data Protection and Ethics and Standards Guidelines** documents below. You will need to print, sign and return the **Administration Access Agreement** document as explained on the form.

5.3 Once you have approval from your Force or Borough Area lead you will need to complete the on line Data Protection training package to complete the approval process. A link will be sent to you by NWN once your approved application form has been received.

5.4 If your police force area or Borough does not have a Neighbourhood Watch Association, please complete the Administration Access Agreement and send it to the NWN Administrator at the address below or scan it to enquiries@ourwatch.org.uk who will process your application.

Annex A

Rules and Conventions for use of the Neighbourhood Alert System

1. The Neighbourhood Alert system shall only be used for lawful purposes in accordance with the GDPR and the Data Protection Act 2018.

2. Administrators will protect the security of personal data they have access to as outlined at **Annex B**.

3. Information held on Alert may not be disclosed to any third party except as governed by the Terms & Conditions.

4. Personal data from the Alert system must not be copied, cut and pasted, entered manually or downloaded onto any other IT system without the explicit, written authorisation of NWN and / or Visav.

5. Information downloaded from Alert as a CSV file should only be used for the purposes of creating a mail-merge for physical letters (not other forms of communication) or extracting anonymised data.

6. Alert should not be accessed via an unsecured wireless connection.

7. Alert should not be accessed via a shared public computer without taking adequate precautions and being aware of the risks.

8. Reports taken from Alert should be anonymised so no personal information about identifiable individuals is disclosed.

9. Messages sent via Alert should conform to the restrictions outlined at **Annex C** and be allocated a Message Type which most accurately reflects the content of the message.

10. Messages sent via Alert should only be allocated Priority 1 in the event of a serious emergency.

11. Messages containing sensitive information should not be propagated as this makes them visible to the general public on various websites.

12. Messages sent via Alert should not contain politically biased information or any discriminatory or inflammatory language.

Annex B

Data Protection

1. Administrators are responsible for the protection of personal data they process on the Alert system and also if it is downloaded from the Alert system onto a computer or other device or printed in hard copy.

2. Reasonable precautions must be taken to protect the privacy of individuals whose data they are processing. Training will be given in Data Protection but below are some of the key points that MSAs must take account of: -

   - Follow general computer security advice – password protect computers and / or files that contain personal data with a strong password and download computer software updates as soon as they are available.

   - Do not store personal data on any computer or other device for longer than necessary for the purpose they are needed.

   - Avoid transporting personal data on a device (e.g. laptop, CD/DVD or USB stick) where possible and take suitable security precautions when this is unavoidable (not leave laptops unattended, keep USB sticks secure etc.).

   - Avoid sending personal data by email.

   - Avoid storing personal data in hard copy. If this is necessary, use a lockable cupboard, cabinet, box etc. and dispose of by shredding or burning so it cannot be re-used.

For more information and guidance on Data Protection please refer to the NWN Data Protection Guidance https://www.ourwatch.org.uk/support/support-associations/set-and-run-association

Annex C

Alert Message Restrictions

1. Do not send messages that relate to:-

   - Sudden Deaths
   - Serious or life-threatening incidents
   - Domestic incidents or crimes
   - Major incidents
   - Covert police operations
   - Police staff / officer disciplinary matters
   - Wanted people
   - Missing people
   - Politics or police force policy

2. Do not post: -

   - Anything that identifies victims, witnesses and / or property without the express permission of your local police force
   - Names or details that could identify someone who has been arrested and / or charged
   - Restricted or sensitive information
   - Copyrighted or branded images
   - Prejudicial language
   - Long lists of crimes with no other supporting information such as crime prevention advice or relevant details of police appeals for information

3. Seek advice from your local Police Press office or Communications Department for corporate guidance in relation to: -

   - Real time updates from ongoing incidents
   - Force-wide initiatives and operations
   - Issues that involve community tension
   - Responses to complex or persistently negative queries

Annex D

Neighbourhood Watch Network

Ethics and Standards Guidelines

Overview

The Neighbourhood Watch movement aims to build safer, stronger and more resilient communities.

To further these aims and to ensure public confidence in Neighbourhood Watch, it is appropriate that Neighbourhood Watch members adhere to these Ethics and Standards Guidelines, and Policies adopted by the Neighbourhood Watch Network.

1. **Honesty and integrity**
You are truthful and trustworthy. You always do the right thing. You will be honest and act with integrity at all times.

2. **Fairness, Respect and Courtesy**
You act with self-control and tolerance, treating everybody with respect and courtesy. You respect the rights of all individuals.

3. **Leadership, Objectivity and Openness**
You lead by good example. You make choices based on facts and your best judgement. You are open and transparent in your actions and decisions.

4. **Selflessness**
You act in the public interest.

5. **Responsibilities and Accountability**
You will be diligent in the exercise of your responsibilities. You are answerable for your decisions, actions and omissions.

6. **Confidentiality**
You will treat information with respect, and in accordance with the law.

7. **Equality and diversity**
You act with fairness and impartiality. You will not discriminate unlawfully or unfairly.

8. **Conduct**
You will behave in a manner which does not bring discredit upon Neighbourhood Watch or Neighbourhood Watch partners or undermine public confidence.