DATA PROTECTION GUIDANCE FOR NEIGHBOURHOOD WATCH ASSOCIATIONS AND NEIGHBOURHOOD WATCH COORDINATORS

CONTENTS

1. BACKGROUND

1.1 A new Data Protection Act is in the process of being drafted by Government. This will incorporate the General Data Protection Regulation (GDPR), approved by European Parliament in April 2016 to come into effect on 25 May 2018. The UK Government have already confirmed that UK's decision to leave the EU will not affect the start of GDPR in the UK.

1.2. This guidance has been developed to assist Force Area/ District / Borough Neighbourhood Watch Associations and Neighbourhood Watch Coordinators to understand the practical implications of the new Data Protection legislation for those who collect, hold and / or use the personal data of their members to manage their Neighbourhood Watch schemes locally.

2. PERSONAL DATA

2.1 Data Protection applies whenever information relating to an identifiable, living individual -"personal data" - is processed, collected, recorded, stored or disposed of.

2.2 GDPR widens the data that the Data Protection Act applies to as it now includes both automated personal data and manual filing systems.

2.3 Personal data collected, held and / or used by Neighbourhood Watch will generally include Scheme Coordinators' and members' names, addresses, phone numbers and e-mail addresses. Whether this information is kept electronically or in hard copy, it must be collected, kept and used in line with the guidance contained below.

3. SPECIAL CATEGORY DATA

3.1 Special category data is more sensitive, and so needs more protection. For example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

3.2 The explicit consent of the person is needed to use any special category data for one or more specified purposes.

3.3 When collecting this data (and any other personal data) it must be made clear to the person what it will be used for. The purpose of NW collecting any special category data - and this will generally be limited to race and ethnicity - is to help Force Area / Borough Associations and Coordinators understand the profile of their members and assist them to target information or focus their engagement, and / or recruitment to reach groups of people who may be under-represented within Neighbourhood Watch in their local area. If you are not intending to use this data for this purpose then then the advice is **not** to collect it.

4. WHO DOES THE GDPR APPLY TO?

4.1 The GDPR applies to 'controllers' and 'processors'. The controller says how and why personal data is processed and the processor acts on the controller's behalf.

4.2 It is important that you establish who has responsibility for deciding what is to be recorded, how the information should be used and to whom it may be disclosed. If you make these decisions, then you are the data controller and you are legally responsible for compliance with the Data Protection Act.

4.3 When a person joins Neighbourhood Watch via the Our Watch website (www.ourwatch.org.uk) or one of the Neighbourhood Watch Force Area microsites developed by Visav Ltd, their details are added to the national Neighbourhood Watch Scheme Register. The Register keeps a record of where Neighbourhood Watch Schemes are, enables people to use the postcode search on the OurWatch website to find and join existing schemes and notifies the coordinator when a person joins their scheme. Neighbourhood Watch Coordinators can also set up their own e-mail distribution lists on this system **with their members' consent** and use this to communicate with their members to avoid keeping separate records. The Neighbourhood Watch Network is a data controller for the data that is held on this Register, though in some circumstances Force Area / Borough associations may also hold this responsibility e.g. if they have purchased their own licence to use the Neighbourhood Alert system. Both the Neighbourhood Watch Network (NWN) and Visav are registered as Data Controllers with the Information Commissioner's Office and take responsibility for how personal data held on the Scheme Register is used and kept secure.

4.4 The Neighbourhood Watch Network recommends that Neighbourhood Watch areas use the secure national Neighbourhood Watch Scheme Register to hold and administer the personal data of their members – or another secure IT system used locally, such as OWL, or a police system that the local NW association and coordinators can access. This gives added protection to Force Area / Borough associations and local coordinators who may use the data by:-

- ensuring the integrity and security of data management processes
- capturing and recording the consent of the person to process their data

- keeping personal data up to date
- giving members the opportunity to update their own details
- ensuring the reliability of those who have access to it
- minimising the risk in holding personal data in hard copy or on spreadsheets or other non- secure electronic formats

4.5 Local Neighbourhood Watch groups, who hold members' data which are not on the Neighbourhood Watch Scheme Register and are not held on other systems controlled by a third party i.e. OWL, the police – will be classed as data controllers. This could be a NW Force / District Area/ Borough Association or, if the data is just held at a very local level, the Scheme Coordinator. The data controller needs to ensure that the processes for managing members' data are compliant with the Data Protection principles. The following section outlines these principles and offers advice on how to comply with them.

5. DATA PROTECTION PRINCIPLES

5.1 The GDPR requires that the controller shall be responsible for, **and be able to demonstrate**, compliance with the data protection principles. **A Quick Checklist** at **Annex A** identifies the main things for Neighbourhood Watch Coordinators and Force Areas/ Boroughs to consider. These principles are:

5.2 Principle 1

Personal data shall be processed lawfully, fairly and in a transparent manner;

5.2.1 The lawful grounds that Neighbourhood Watch Network, Force Area/Borough Associations and local Neighbourhood Watch Schemes have for collecting and using the personal data of members is **the consent** of the person about whom the data is held.

5.2.2 Perhaps the most significant of GDPR's impacts is the changes to the requirement for collecting people's consent to processing their data. GDPR requires 'freely given, specific, informed and unambiguous consent' indicated 'either by a statement or by a clear affirmative action' and explicitly states that "silence, pre-ticked boxes or inactivity" will be inadequate to infer someone's consent.

5.2.3 You need to have a person's **consent** when you use their personal data – i.e. using their name and address for the purposes of contacting them. However, if you deliver a newsletter to every home in the village or street without using or collecting personal information about the people to whom the newsletter is delivered, Data Protection legislation **does not apply** and you do not need everyone's consent to do this.

5.2.4 The GDPR also introduces a requirement that the consent of each of your **new** members for you to hold and use their personal data **can be demonstrated** – either by capturing it electronically on the Neighbourhood Watch Scheme Register or by some other electronic or manual means.

5.2.5 The data controller (the scheme coordinator, Force Area / District / Borough association or NWN) is responsible for demonstrating compliance with this and the other Data Protection Principles outlined below. From 25th May 2018 a record of all **new** members' consent to use their data should be obtained showing when the consent was obtained and for what purpose and kept in either a hard copy or electronic format that should be retained securely. The national Neighbourhood Watch Scheme Register will record this consent if the person registers as a member via the OurWatch website or one of the local microsites developed by Visav. The accompanying **template** could be used as an alternative if necessary and can be adapted to include consent to share and receive information from other Information Providers currently available in your local area via the Alert (or other) system.

5.2.6 If members consent to receive information from both their local Neighbourhood Watch group and Neighbourhood Watch Network then you can either invite them to register on the OurWatch website or alternatively set up your own e-mail distribution list on the Neighbourhood Alert or other messaging system locally and forward national newsletters and other Neighbourhood Watch Network communications to members in this way.

5.3 Principle 2

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

5.3.1 The purpose of collecting and processing personal data of Neighbourhood Watch members is the organisation and running of Neighbourhood Watch Schemes. When people share their personal data when joining Neighbourhood Watch, they should be informed who has access to the data and for what purpose. As a minimum, the person supplying their data should be advised of:

- Who the data controller is
- What they are going to do with their information
- Who it will be shared with
- That their personal data will not be shared with anyone else or for any other purpose without their explicit consent

5.3.2 This information should be included as part of any hard copy or electronic process that a new member completes to join your Scheme. (See accompanying **template**)

5.4 Principle 3

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

5.4.1 Identify the **minimum** amount of personal data you need to properly run your Neighbourhood Watch scheme. You should hold that much information, and no more.

5.4.2 You may need to understand the diversity of your members to understand how representative they are of the local population in terms of age and ethnicity. This can assist you to target recruitment and new schemes to address any gaps you identify. You may therefore wish to include an optional section in your registration process that enables people to identify their age and ethnicity to help you to do this.

5.4.3 Bear in mind though, that if you do collect data about the race and ethnicity of your members that this is special category data (see 3.1) and the explicit consent of the person is needed to use this data. You need to make it clear at the point of collection why you are asking for this data and how you will use it and give the person the option to opt-in to sharing it for that purpose.

5.5 Principle 4

Personal data shall be 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

5.5.1 The data controller is responsible for:

- Regularly reviewing the data held about members to check its accuracy and keep a note of when this is done. Once every couple of years should suffice.
- Giving members a means of updating their details – even if this is simply ensuring that all members have relevant contact details of the person managing their data so they can advise them of any changes.
- Ensuring people's details are updated as soon as possible after notification of any changes and keeping a note of when they were updated.

5.5.2 It is recommended that the personal data of members held by Force/ District Area / Borough Associations and Neighbourhood Watch coordinators be reviewed as soon as practicable (if this hasn't been done recently) to check the accuracy of the personal data that you hold and update it if necessary.

The accompanying **template** can be adapted to update the data of existing members.

5.6 Principle 5

Personal data shall be 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;

5.6.1 People should be given the opportunity to withdraw their consent for the use of all or any part of the data held on them at any time. GDPR introduces the "right to be forgotten" – so if someone wishes all their data to be deleted then you need to comply with their wishes.

5.6.2 It is also important to remember that personal data should be deleted as soon as it is no longer relevant. Let people know what to do if they choose to leave your Neighbourhood

Watch Scheme or move away. Information about this could be included as part of the process when people first sign up to your scheme and / or made clear on your website and in local communications.

5.6.3 If your Neighbourhood Watch Scheme ceases to operate, ensure there is a process to let all your members know. Give them the option to start or join a new or neighbouring Scheme if they so wish, to remain as a member of Neighbourhood Watch on the national Neighbourhood Watch Scheme Register or delete or have their data deleted from any electronic or hard copy files.

5.6.4 When updating people's details, delete the previous data. Don't keep old versions of spreadsheets or lists as it is easy to lose track of which is the most up to date.

5.7 Principle 6

Personal data shall be 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.

5.7.1 Physical security

Take steps to ensure that the location where you keep or access people's personal data is secure enough to prevent unauthorised access to it i.e. adequate home security measures and locked drawers or cabinets to keep hard copy records. Similarly, take particular care to ensure the security of any hard copy documents or mobile devices containing personal data that you take outside your home or office. Dispose of any paperwork containing personal data so it cannot be re-used i.e. by shredding or burning hard copies.

5.7.2 Computer security

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 use public Wi-Fi to access files or systems containing people's personal data. Further online security advice is available at https://www.cyberaware.gov.uk/ and on the OurWatch website https://www.ourwatch.org.uk/knowledge/scams-fraud/ .

Dispose of any old computers containing personal data so it cannot be re-used i.e. by wiping or ideally destroying hard drives.

5.7.3 Staff / Volunteers

The Data Protection Act requires data controllers to take reasonable steps to ensure the reliability of any individuals who have access to personal data and that they understand

the importance of protecting personal data. This is particularly important when nominating volunteers as Multi Scheme Administrators.

Individuals who have access to personal data need to understand:

- The duties of your Association or Scheme under the Data Protection Act and restrictions on the use of personal data
- Their individual responsibilities for protecting personal data, including the possibility that they may commit criminal offences if they deliberately try to access, or to disclose, information without authority
- Proper procedures to use to identify callers
- Dangers of people trying to obtain personal data by deception (for example, by pretending to be the person whom the information is about or by making "phishing" attacks) or by persuading you to alter information when you should not do so
- Any restrictions placed on the use of personal computers (to avoid, for example, virus infection or spam)

6. PAYING A DATA PROTECTION FEE TO THE ICO

6.1 Under the 2018 Regulations, data controllers must pay the ICO a data protection fee unless they are exempt.

6.2 A specific exemption applies to bodies or associations that are not established or conducted for profit. However, the exemption applies only if:

- you are only processing data for the purposes of establishing or maintaining membership or support for a body or association not established or conducted for profit, or providing or administering activities for individuals who are members of the body or association or have regular contact with it
- you only hold information about individuals whose data you need to process for this exempt purpose
- the personal data you process is restricted to personal information that is necessary for this exempt purpose

If yes to all – a data protection fee is not due

6.3 If you are still not sure, or need any further general advice about Data Protection issues then the ICO recommend you contact them on their helpline number for small organisations - 0303 123 1113.

7. CCTV

7.1 The use of CCTV cameras for limited household purposes can be exempt from the Data Protection Act under S36 - "Personal data processed by an individual only for the purposes

of that individual's personal, family or household affairs (including recreational purposes)"

7.2 New ICO Guidance revokes the previous requirement for householders to register / pay a fee if a camera faces outwards from an individual's private domestic property and captures images of individuals beyond the boundaries of their property. The new guidance states that if you use CCTV for household purposes, even if capturing images beyond the boundaries of the property you do not have to pay the fee.

https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf

8. DATA BREACH NOTIFICATIONS REQUIREMENTS FOR ALL CONTROLLERS AND PROCESSORS

8.1 A personal data breach is more than just losing personal data. It means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

8.2 The data controller must notify the Data Protection Authority within 72 hours of its discovery of a breach, **unless** the controller can demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of individuals, for example, in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. The controller is also required to notify affected people if the breach is likely to result in a high risk to them.

8.3 If you discover that personal data that you control at either a force / district / borough area or at street level has been destroyed, lost, altered, disclosed to a third party or accessed without authority you must decide whether there is a likelihood that this will result in a risk to the rights and freedoms of individuals as outlined above, taking into account the circumstances under which the breach occurred and the type of data involved.

8.4 If your Force Area / Borough association or Neighbourhood Watch group experience a data breach and feel that any of the above rights and freedoms are likely to be at risk as a result of the breach, contact the ICO to report the breach within 72 hours outlining: -

- the nature of the personal data breach – including categories of individuals concerned and approximate numbers; and categories of data records involved and approximate numbers;
- the name and contact details of the Data Protection Officer (if applicable) or other contact point;
- a description of the likely consequences of the breach; and

- a description of the measures taken or proposed to deal with the breach, and to mitigate potential adverse effects.

8.5 If you are not sure, NWN can assist you to ascertain whether the risk is such that the breach needs to be notified. Please contact the NWN office on **0116 4026111** as soon as you discover the breach.

9. PROCESSING AND DISCLOSURE OF PERSONAL DATA

9.1 The justification for householders collecting and using personal data and CCTV footage that may assist to identify offenders is that it is "necessary for the purposes of the prevention or detection of an unlawful act …" This information should only be shared with the police or another relevant law enforcement body, such as the local authority – e.g. in the case of fly tipping etc.

9.2 NWN strongly recommends that you do not share information on social media or by other means that could enable a person you suspect to be responsible for an offence to be identified either from a photograph, a car registration number, CCTV footage or by naming them, unless this information has been supplied and / or approved by the police to share in this manner.

9.3 Doing so could jeopardize any police investigation, particularly if an identification parade is subsequently held in relation to the crime, could put you at risk of recrimination by suspected offenders or their families or friends or lead to a complaint or legal action against you by the person identified. If incorrect or misleading information about crimes and suspected offenders is shared in this way it also has the potential to negatively impact upon the reputation and future trust in the Neighbourhood Watch movement.

9.4 Any repercussions from such activity will not be covered under the Public Liability Insurance currently offered to Neighbourhood Watch schemes by Neighbourhood Watch Network.

10. DIRECT MARKETING

10.1 Direct marketing covers the promotion of aims and ideals as well as the sale of products and services. This means that the rules will cover not only commercial organisations but also not-for profit organisations (e.g. charities). In many cases organisations will need consent to send people direct marketing.

10.2 Neighbourhood Watch newsletters, especially if they are sponsored by local companies, may contain marketing material promoting local services. To demonstrate that recipients' consent to receive this material has been knowingly and freely given, the ICO recommends that opt-in boxes are used and that clear and specific records of consent

should be kept. This information could be included as part of any hard copy or electronic process that a new member completes to join your Scheme. (**See attached template**).

10.3 Organisations must stop sending direct marketing messages to any person who objects or opts out of receiving them.

A QUICK CHECKLIST

Annex A

See paragraph ref. for further information

1. Do I hold and manage contact details for my scheme members? (4.2)

2. Do I need all the information that I keep about members? (2.3, 3.3 & 5.4)

3. Do the people whose information I hold know that I've got it and consent to it being used for Neighbourhood Watch purposes? (5.2.)

4. Are members likely to understand what their data will be used for and who will have access to it? (5.3)

5. Do I have a way of demonstrating that members consent to their data being used in this way going forward? (5.3)

6. Do I have a process for ensuring the personal information I hold is accurate and up to date? (5.5)

7. Do I have a process for deleting/destroying personal information as soon as it is outdated, I have no further need for it or the person asks that I do so? (5.6)

8. Am I satisfied the information is being held securely, whether it's on paper or on a mobile device or computer? (5.7)

9. Is access to personal information limited only to those who need to know it? (5.7.3)

10. Do I and volunteers who manage membership data understand our individual responsibilities for protecting personal data? (5.7.3)

11. If I or my members use CCTV that monitors beyond the boundaries of their property, are they registered with the Information Commissioner's Office? (7.4)

12. Is personal information shared in line with this guidance? (9)

13. Do I know what to do in the event of a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data? (8)