The London Borough of Sutton Neighbourhood Watch Association
Registered Charity No. 1120448

WORKING ARRANGEMENTS IN SUPPORT OF THE DATA PROTECTION POLICY

These Working Arrangements were updated on 21 May 2018

Storing Personal Data

Hard (paper) copies of personal data will be kept to a minimum and kept safe from loss or theft of document or data.

Electronic (digital) records of personal data will be kept to a minimum, only stored on secure devices and will be protected from the unwanted actions of unauthorised users, such as a cyber attack or a data breach.

Such data will be password protected and or encrypted to prevent any unauthorised access and will only be shared on a need to know basis.

Destroying Personal Data

- When complying with the policy all Digital or Hard (paper) copies of personal data will be either destroyed or redacted.
  A record will be kept of when such data was destroyed/redacted.
- For administration and to accommodate Subject Access Requests, hard (paper) copies of membership applications will be kept for a minimum of 3 months and a maximum of 6 months from the date of enrolment.
- Any person with access to personal data upon leaving membership:
  - Will have their access stopped.
  - Will pass their records to their successor or the Association Secretary as directed.
  - Any Digital or Hard (paper) copies of personal data remaining in their possession will be destroyed.

Compliance with the Data Protection Policy and the Working Arrangements in Support of the Policy

All who are granted access to members personal data must agree to comply fully with the Data Protection Policy and the Working Arrangements in Support of the Data Protection Policy.

Access to Personal Data

Access to personal data is on a strictly need to know basis regardless of role.

Full Access v/v Partial Access is determined by the actual data necessary to carry out a particular role or task. Such access should be withdrawn upon completion of the task.

As examples:

- Ward Co-ordinators WILL be granted FULL access to personal data about the members in their Ward. This access may be extended to an approved deputy whose duties require full access.
- Street Coordinators MAY be granted PARTIAL access to personal data about the members in their Watch. In this instance access would be limited to minimum contact details.
- The police should normally only have access to contact details.

The person granting access is responsible for ensuring that the level of access is necessary and that the person being granted access agrees to comply fully with the Data Protection Policy and the Working Arrangements in Support of the Data Protection Policy.

Personal Data

Personal data held by the Association are Names, Telephone Numbers and Email Addresses.

- Names and telephone numbers are personal
- Email addresses in isolation are not personal. However in a list of members they become personal, because a third party will know that the account holder is a NHW member.
- Addresses are not personal unless associated with names or other contact details.
- A list of members' addresses (even without names) becomes personal, because a third party will know that the resident is a NHW member.
- Membership numbers unless associated with Names, Telephone numbers or Email addresses are not personal.

Subject Access Requests

Subject access requests (requests for copies of personal data from individuals) will be responded to within one calendar month. A record will be kept of how and when we responded.

Data Breaches

Any member who becomes aware of or suspects a data breach (i.e. an unauthorised person has obtained access to personal data), must immediately report it to the Association Chair and Secretary and do all they can to prevent any further breach.