NRA Risk Assessment for Security of Data

Northwood Residents Association (the NRA) is a non-political, non-commercial, non-profit unincorporated association set up to inform and safeguard the interests of its members. The minimum personal and non-personal members' data for this purpose is held securely by the NRA. This includes members postal address with annual subscription payment history, plus name, email address and telephone number where optionally provided.

The NRA ensures "appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, any such data." This is the purpose of the Annual Risk Assessment conducted by the NRA DPO (Data Protection Officer).

NRA Data Risk Assessment approach

The Risk Assessment looks at:
What data is held? Is all data held necessary? Who has access to that data? How securely is the data held? What impact results from any data security breach?

Data Security Assessment

1. **What data is held for members and officers? Is all data held necessary?**
   a. Postal address. Essential to establish membership status and permit communication
   b. Member name. Not essential, but desirable for communication by officers and delivery of Newsletters
   c. Subscription history. Essential to establish membership and for officers to issue reminders
   d. Email address. Optional – a convenient way for the NRA to alert members to matters of local interest and remind when subs are due. Despite their email addresses being recorded, members have the right to opt-out for a period of 24 months from receipt of such general alerts.
   e. Member telephone number. Optional – a convenient way for NRA officers to contact local members.

2. **Who has access to that data?**
   a. Members' and officers' data is held on a proprietary membermojo (mmjo) database.
   b. Neither the public nor members have full direct access to this data on the NRA website.
   c. Chief Road Steward (CRS) is the main mmjo Administrator and solely can award access authority.
   d. Several officers have password-protected access to read but not necessarily enter or amend this data.
   e. CRS, Treasurer, Membership Secretary and Website Manager have entry or amend authority.
   f. Officers with read-only authority are NRA Chairman, Secretary, Editor and IT Manager.
   g. Road Stewards (RS) and their co-ordinating Area Road Stewards (ARS) are provided a confidential link by which to access only membership addresses and status information (updated weekly) re their assigned "patches" essential for collection of annual subscriptions, and distribution of information by Newsletter three times a year.

3. **How securely is the data held? And for how long?**
   a. All membership data is held securely on mmjo.
   b. Some NRA officers can read and / or update this data by password-protected access as described above.
   c. If any NRA officers wish to store any NRA member data locally, they are required to password-protect such data when downloaded to their own electronic devices as dictated by the NRA Privacy policy document issued to them. If they wish to print or copy any such data to paper records, they are required to take reasonable precautions to keep such copied data secure.
   d. Data on the members' database shows current subscription contributions and for the previous two years, but CRS as main mmjo administrator keeps a secure archive of past, downloaded, mmjo data.
   e. Provision exists for address data to show change of resident membership by creating a new database record, in which case prior resident data records can be securely stored for a maximum of 6 years via the downloaded mmjo archive, and previous custom database.
   f. The NRA Treasurer keeps their own membership subscription records securely for the sole purpose of producing Annual Financial reports for the Association, which are independently audited ahead of each Annual General Meeting.

4. **What impact results from any data security breach?**
   a. No members' age, race or ethnicity data is held – so there is zero risk on this account
   b. The only members' financial data held is their historic annual subscription contributions, typically ranging from the previous minimum £2 (now £3) to sometimes £20 – so there is zero risk on this account
   c. Identity theft / impersonation from a data breach on the whole database is judged very low as data content such as member names at each address along with telephone and email addresses (if optionally provided) is available from many other sources and is not comprehensive enough for impersonation.
   d. Risk of data breach impact on data correctly downloaded by officers is similarly judged extremely low.

5. **Personal responsibility**
   It is the responsibility of all those accessing personal data to ensure that security is treated seriously. Those involved will be routinely made aware by NRA DPO (Data Protection Officer) - who is currently CRS - of this risk assessment and are required to agree to comply with the relevant measures/actions.

Annual NRA data risk assessment above completed by its DPO (currently Paul Barker) 13th September 2025