Risk Assessment for Security of Data

Northwood Residents Association (the NRA) is a non-political, non-commercial, non-profit 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
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 custom-designed database on the NRA website
b. Neither the public nor members have direct access to this data on the NRA website.
c. All officers have authority-level password-protected access to read but not necessarily enter or amend this database.
d. Officers are NRA committee members, webmaster and website designer / maintainer, plus Road Stewards (RS) and their co-ordinating Area Road Stewards (ARS) needing membership status information for collection of annual subscriptions and distribution of information by Newsletter three times a year.
e. Chief Road Steward (CRS), Membership Secretary and Treasurer have password-protected access to add and update all membership data on the database.
f. RS can elect to have password-protected access to review and update membership data for any road for which they have material distribution and subscription collection authorisation.
g. ARS can elect to have password-protected access to review and update membership data for any RS for whom they have supervisory and distribution authorisation.

3. How securely is the data held? And for how long?

a. All membership data is held securely by the webmaster and designer on a website hosted for the purpose.
b. All NRA officers can access and / or update this data by authority-level password-protected access as described above.
c. If 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. 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 three years.
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 are securely stored for a maximum of 6 years.
f. The NRA Treasurer keeps his 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 minimum £2 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 of this risk assessment and agree to comply with the relevant measures/actions.

Annual NRA data risk assessment above completed by its DPO (currently Paul Barker) 6th June 2018