RADLEY GOOD NEIGHBOURS

Confidentiality and Data Protection Policy

Document Purpose

This document describes the RGN policy for ensuring that all Client, Volunteer and Committee Member information is kept secure and confidential.

Principles

a. In order to discuss issues and seek advice, Volunteers may share information with any Radley Good Neighbours Committee Member, and Committee Members may share information between themselves.
b. Everyone in RGN will avoid exchanging personal information or comments about Clients. It is not appropriate, for example, to discuss a person's sexuality or personal circumstances without their prior consent.
c. Everyone in RGN will avoid disclosing information about individuals in social settings.
d. Volunteers will not disclose to anyone other than an RGN Committee Member any Client information considered sensitive, personal, financial or private without the knowledge or consent of the Client.
e. Where there is a legal duty on RGN to disclose information (for example, where abuse is suspected), the person will be informed that disclosure has or will be made.

Why information is held

a. Information held by RGN relates to Volunteers, Clients, points of contact and other services which support or fund the group.
b. Information is kept to enable RGN to offer an appropriate service to its Clients.
c. Anonymous aggregated data about age, gender, ethnicity, disability and employment status of Clients may be kept for the purposes of monitoring the RGN equal opportunities policy and also for reporting back to funders.
d. RGN Volunteers and Clients shall be informed that the RGN Committee intends to hold information about them both electronically and on paper.

Access to information

a. Information about a Volunteer or Client should only be shared with a Volunteer or Committee Member who is working directly with that person.
b. Clients and Volunteers are entitled to see information held in their name.
c. Access to any electronic information will be password protected, with passwords only known to the RGNS Committee. This includes information held by a third party (e.g. OCC DBS database) and information held on the RGN laptop.

Storing information

a. All printed confidential information shall be kept in a secure place such as a filing cabinet, desk drawer, etc.
b. All electronic information shall be stored on-line in a secure facility such as Dropbox. Access shall only be made available to Committee Members.
c. Any computer linked to Dropbox or holding personal data shall be secure, should not visible from outside and – if possible - kept in a locked room or cabinet.
d. Any memory stick holding personal data shall be stored in a secure location such as a filing cabinet or desk drawer.

Duty to disclose information

There is a legal duty to disclose some information including:

- Abuse of Vulnerable Adults, which will be reported to the Social Services Department
- Drug trafficking, money laundering, acts of criminality (such as terrorism or treason), which will be disclosed to the police.

DBS Disclosures

a. As an organisation using the Disclosure and Barring Service (formerly CRB) to help assess the suitability of volunteers for positions of trust, the RGN shall comply fully with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.
b. Disclosure information is kept securely, in lockable storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.
c. In accordance with section 124 of the Police Act 1997, Disclosure information is only passed to those who are authorised to receive it in the course of their duties.
d. Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.
e. Once a decision has been made on an applicant, Disclosure information is kept for no longer than is necessary. This is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints.
f. Once the retention period has elapsed, any Disclosure information will immediately be destroyed by secure means, e.g. shredding, pulping or burning. Photocopies or other images of the Disclosure, or any copy or representation of the contents of a Disclosure, will not be kept. However, a record of the date of issue of a Disclosure, the name of the subject, the unique reference number of the Disclosure and the details of the recruitment decision taken will be kept.

Data Protection Act

Information about individuals, whether held electronically or on paper, falls within the scope of the Data Protection Act and shall comply with the following principles which state that data must be:

- Obtained and processed fairly and lawfully.
- Held only for specified purposes.
- Adequate, relevant and not excessive.
- Accurate and up to date.
- Not kept longer than necessary.
- Processed in accordance with the Act.
- Kept secure and protected.
- Not transferred out of Europe.

The RGN Committee undertakes to comply with these data protection principles

Breach of confidentiality

Any Volunteer or Committee Member who breaches any of the conditions within this policy will be dismissed from the RGN.