Race Against Dementia

Data Protection Policy

February 2023

Review Date: April 2024

Introduction

The security and management of data is important to ensure that Race Against Dementia (RAD) can function effectively and successfully for the benefit of those who use our services.

In doing so, it is essential that people's privacy is protected through the lawful and appropriate use and handling of their personal information.

The use of all personal data by RAD is governed by:

- The General Data Protection Regulation (GDPR)
- The UK Data Protection Act 2018 (DPA)
- The Privacy and Electronic Communications Regulations (PECR)

Every member of staff has a responsibility to adhere to the Data Protection Principles outlined in the GDPR, and to this Data Protection Policy. Other relevant policies include the Confidentiality Policy and Privacy Statement.

If you have a question about this Data Protection Policy or an area of concern about data protection matters, please contact the Data Protection Officer (DPO), currently Jan Knight jan@raceagainstdementia.com.

Data Protection Principles

There are six Data Protection Principles defined in Article 5 of the GDPR. These require that all personal data be:

- processed in a lawful, fair and transparent manner;
- collected only for specific, explicit and limited purposes ('purpose limitation');
- adequate, relevant and not excessive ('data minimisation');
- accurate and kept up-to-date where necessary;
- kept for no longer than necessary ('retention');
- The Data Processing Register will be reviewed at least every six months by the DPO;
- handled with appropriate security and confidentiality.

RAD is committed to upholding the Data Protection Principles. All personal data under our control must be processed in accordance with these principles.

Lawful Processing

All processing of personal data must meet one of the six lawful bases defined in Article 6(2) of the GDPR:

- Where we have the consent of the data subject;
- Where it is in our legitimate interests and this is not overridden by the rights and freedoms of the data subject;
- Where necessary to meet a legal obligation;

- Where necessary to fulfil a contract or pre-contractual obligations;
- Where we are protecting someone's vital interests;
- Where we are fulfilling a public task or acting under official authority;

Any special category data (sensitive types of personal data as defined in Article 9(1) of the GDPR) must further be processed only in the line with one of the conditions specified in Article 9(2) Processing of special categories of personal data.

The most appropriate lawful basis will be noted in the Data Processing Register (see Section on Accountability below).

Where processing is based on consent, the data subject has the option to easily withdraw their consent.

Where electronic direct marketing communications are being sent, the recipient should have the option to opt-out in each communication sent and this choice will be recognised and adhered to by us.

Data Minimisation and Control

Data collection processes will be regularly reviewed by the DPO to ensure that personal data collected and processed is kept to a minimum.

RAD will keep the personal data that it collects, uses and shares to the minimum amount required to be adequate for its purpose.

Where RAD does not have a legal obligation to retain some personal data, we will consider whether there is a business need to hold it.

RAD will retain personal data only for as long as it is necessary to meet its purpose.

In the case of sharing personal data with any third party, only the data that is necessary to fulfil the purpose of sharing will be disclosed.

Accountability

The DPO has the specific responsibility of overseeing data protection and ensuring that RAD complies with the data protection principles and relevant legislation (see Role of the DPO below).

The DPO will ensure that RAD's Data Processing Register is kept up to date and demonstrates how the data protection principles are adhered to by RAD. Individual members of staff have a duty to contribute to ensure that the measures outlined in the Register are accurately reflected in RAD's practice.

The Executive Committee monitors our compliance with relevant policies and regulatory requirements in respect of data protection as part of our Data Management Strategy.

All employees, regular volunteers, consultants, partners or other parties who will be handling personal data on behalf of RAD will be appropriately trained and supervised where necessary.

The collection, storage, use and sharing of personal data will be regularly reviewed by the DPO.

Where there is likely to be a high risk to individuals rights and freedoms due to a processing activity, RAD will first undertake a Data Protection Impact Assessment (DPIA) and consult with the Information Commissioner's Office (ICO), prior to processing, if necessary.

Use of Processors

RAD must only appoint processors who can provide sufficient guarantees around compliance with the GDPR and that the rights of data subjects will be protected.

Where a processor can demonstrate that they adhere to approved codes of conduct or certification schemes, this should be taken into consideration for choice of supplier.

Where RAD uses a processor, a written contract with compulsory terms as set out in Article 28 of the GDPR must be in place (plus any additional requirements that RAD determines). Processors can only act on the written instruction of RAD.

Organisational Measures

All devices owned by RAD will have hardware encryption set up by default where possible, including laptops, mobile devices and removable media.

All staff, contractors, temporary workers, consultants, partners or anyone else working on behalf of RAD and handling personal data are bound by the data protection legislation and this Policy.

Where any contractor, temporary worker, consultant, or anyone else working on behalf of RAD fails in their obligations under this Policy, RAD may ask that they indemnify RAD against any cost, liabilities, damages, loss, claims or proceedings that may arise from that failure.

The Role of the Data Protection Officer

The DPO role is assigned to a member of staff on a voluntary basis i.e. RAD is not legally obliged to have a DPO. RAD has chosen to do so as part of demonstrating its accountability and ensuring its compliance with data protection requirements.

The DPO assists RAD to:

• monitor RAD's internal compliance;
• inform and advise on RAD's data protection obligations;
• provide advice regarding Data Protection Impact Assessments;

• act as a contact point for data subjects and the Information Commissioner's Office.

The DPO is easily accessible as a point of contact for staff for data protection issues and is identified as the point of contact in our Privacy Notice and other external material.

The DPO identifies, organises and delivers training for staff and meets with new staff during their induction to discuss data protection matters, including this Policy.

The DPO is responsible for carrying out responses to requests made by data subjects, reporting breaches and drawing up policies and procedures. This does not preclude another responsible member of staff from carrying out these duties.

Rights of Data Subjects

Under data protection laws, data subjects have certain rights:

- Right to be informed. The right to be told how their personal data is used in clear and transparent language;
- Right of access. The right to know and have access to the personal data we hold about them;
- Right to data portability. The right to receive their data in a common and machine-readable electronic format;
- Right to be forgotten. The right to have their personal data erased;
- Right to rectification. The right to have their personal data corrected where it is inaccurate or incomplete;
- Right to object. The right to complain and to object to processing;
- Right to purpose limitation. The right to limit the extent of the processing of their personal data;
- Rights related to automated decision-making and profiling. The right not to be subject to decisions without human involvement.

RAD will uphold individuals' rights under data protection laws and allow them to exercise their rights over the personal data we hold about them. Privacy information will acknowledge these rights and explain how individuals can exercise them. Most rights are not absolute, and the individual will be able to exercise them depending on the circumstances, although exemptions may apply in some cases.

Any request in respect of these rights should preferably be made in writing to info@raceagainstdementia.com, but in exceptional circumstances RAD will also accept verbal requests.

There is no fee for facilitating a request, unless it is 'manifestly unfounded or excessive', in which case RAD may seek to recover administrative costs.

Requests that are 'manifestly unfounded or excessive' can be refused.

RAD will take reasonable measures to require individuals to prove their identity where it is not obvious that they are the data subject.

RAD will respond to the request within one month from the date of request or being able to identify the person, unless it is particularly complex (in which case RAD will respond in no longer than 90 days).

The DPO will ensure that required actions are taken and that the appropriate response is facilitated within the deadline.

The DPO will draw up procedures for responding to requests where necessary, for example, for facilitating Subject Access Requests.

Reporting of Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All members of staff should be vigilant and able to identify a suspected personal data breach. A breach could include:

- loss or theft of devices or data, including information stored on USB drives or on paper;
- hacking or other forms of unauthorised access to a device, email account or the network;
- disclosing personal data to the wrong person, through wrongly addressed emails or bulk emails that inappropriately reveal all recipients email addresses;
- alteration or destruction of personal data without permission.

Where a member of staff discovers or suspects a personal data breach, this should be reported to the DPO as soon as possible.

Where there is a likely risk to individuals' rights and freedoms, the DPO will report the personal data breach to the ICO within 72 hours of the organisation being aware of the breach.

Where there is also a likely high risk to individuals' rights and freedoms, RAD will inform those individuals without undue delay.

The DPO will keep a record of all personal data breaches reported and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.

Appendix

Main policy points:

To help protect people's personal data keep to these Dos and Don'ts:

- Always treat people's personal information with integrity and confidentiality;
- Know what the data protection principles are and apply them;
- Store hard copies securely;
- Use SharePoint to store and share data where needed;
- You have an organisational email address and remote access. Use it rather than sending data to your personal email;
- Be alert to cyberattacks and report suspicious emails or calls to the DPO;
- Report losses of data or devices as soon as possible;
- Before sending direct marketing, ask the DPO if this is appropriate;
- Take care to use the 'bcc' option for bulk emailing;
- Beware of autocomplete on email. Check you are sending to the right email address.
- Do not use personal devices for work-related activity.
- If you have a question about any data protection issue, ask the DPO.

Procedures for staff

While this Policy helps RAD to demonstrate how it seeks to comply with data protection legislation and be accountable for its actions, all members of staff must comply with these procedures for processing or transmitting personal data. In addition, staff should be aware of and adhere to policies around the acceptable usage of computers and any other guidance issued in relation to cyber security and the use of personal data.

- Always treat people's personal information with integrity and confidentiality. Do not hand out personal details just because someone asks you to.
- Where personal data exists as hard copy, it should be stored in a locked box, drawer or cabinet, and not left where anyone could access it.
- Staff have access to the secure document management system SharePoint for the storage of personal data or sensitive information. No removable media devices should be used to transfer these types of information without permission from the DPO or CEO.
- The loss or theft of any device should be reported as soon as possible to the DPO or CEO.
- Take care when connecting to public wi-fi connections, as these can expose your connection to interception. If you are not sure if a connection is secure, do not connect to it.
- If you are thinking of sending marketing to individuals, consult with the DPO first, as there are certain laws that apply to electronic direct marketing. This could include anything that promotes the aims or purpose of RAD, including promoting an event or seeking engagement.

- Take care to email the intended recipient (especially where email address auto-complete is turned on). Use the ‘bcc’ field for emailing several people where using ‘to’ or ’cc’ is not needed.
- These procedures and this policy also applies to the use of remote access to RAD cloud systems. If you are using your own device to access personal data on Office365 (e.g. Outlook or SharePoint), ensure that your device has a firewall and is password protected.
- If you do have a question or are unsure about any of these procedures, contact the DPO or the CEO.