Data Protection Policy

Reference: POL5

Authorised by: Trustees

Reviewed by Trustees 19th September 2018

This policy is operational from 25 May 2018

Reviewed by Trustees October 2020

Contents

1. Purpose

The purpose of this policy is to ensure that RAD operates in compliance with the General Data Protection Act 2018. RAD aims to adhere to the eight principles set out in the Act to ensure that all data collected is dealt with appropriately.

2. Scope

This policy applies to personal and sensitive data which RAD collects, retains and uses. This can include data on staff, trustees, volunteers, clients, members, partners and individuals or organisations that are connected to RAD and its work.

3. Definitions

Data controller - determines the purposes and means of processing personal data.
Data processor - is responsible for processing personal data on behalf of a controller.
Personal data – Data about living individuals that enable them to be identified – e.g. name and address. It does not apply to data about companies and agencies.
Special categories of personal data (previously sensitive personal data) - personal data which the GDPR says is more sensitive, and so needs more protection. The special categories now specifically include genetic data, and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included in special categories of personal data, but similar extra safeguards apply to its processing.

4. References

Data Protection Act 2018.

http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

(accessed 18 July 2018).

A Guide to the General Data Protection Regulation (GDPR). https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

(accessed 18 July 2018).

5. Procedure

5.1 The Principles of Data Protection

The GDPR sets out seven key principles which RAD will act in accordance with. Data will be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for

which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals Integrity and confidentiality;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition there is a new accountability principle. This specifically requires organisations to take responsibility for complying with the principles, and RAD will therefore have appropriate processes and records in place to demonstrate compliance. This will include:

- Briefing the board on Data Protection responsibilities
- Reviewing the Data Protection Policy and related policies
- Advising staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Handling subject access requests (see Appendix B – Subject Access Request Procedure)
- Reviewing contracts with Data Processors
- Ensuring data is stored securely
- Maintaining a data audit
- Reporting breaches to the Information Commissioners Office and the relevant Data Subject(s)

Accountability also includes ensuring that:

persons collecting data understand that they are responsible for following good data protection practice (Refer to Appendix A – Data Protection Responsibilities)

persons collecting and processing data are appropriately trained to do so,

all staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them. Significant breaches of this policy will be handled under the Company's disciplinary procedures which may amount to gross misconduct.

5.2 Data Responsibilities

The GDPR applies to both data controllers and data processors. RAD may act as either a controller or processor within its operations.

RAD is not required to have a Data Protection Officer but RAD's CEO assisted by the

senior management team will lead on RAD's Data Protection Strategy. Individual Project Leads and Officers are responsible for controlling data within their area of work. In addition RAD will take a whole organisation approach where all members of staff are expected to commit to putting data protection at the heart of all RAD's work.

5.3 Disclosure to Third Parties

RAD may share data with other agencies such as local authorities, funding bodies and other voluntary and community sector bodies. The individual will be made aware when providing data how and with whom their data may be shared. There are circumstances where the law allows RAD to disclose data (including sensitive data) without the data subject's consent. These are:

- Carrying out a legal duty as authorised by the Secretary of State,
- Protecting vital interests of an individual or another person,
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights.

5.4 Individuals' Personal Data rights

RAD ensures that the rights of individuals about whom data is held, can be fully exercised under the Act. The GDPR provides the following rights for individuals:

a) The right to be informed
b) The right of access
c) The right to rectification
d) The right to erasure
e) The right to restrict processing
f) The right to data portability
g) The right to object
h) Rights in relation to automated decision making and profiling.

RAD will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected face to face, by telephone or by completing a form or online survey. When collecting data, RAD will ensure that the individual clearly understands the purpose for which data may be used by providing a relevant privacy notice.

All individuals have the right to access their data held by RAD. RAD will take reasonable steps to ensure that this data is kept up to date.

5.5 Data Storage

Data and records relating to individuals will be stored securely and will only be accessible to authorised personnel. Data will be stored for only as long as it is needed

and will be disposed of appropriately. Individuals are advised of the data retention period relevant to them via the appropriate privacy notice.

It is RAD's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation which has been passed on/sold to a third party.

5.6 Data breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. This will be done within 72 hours of becoming aware of the breach, where feasible. When a personal data breach has occurred, RAD will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk the ICO will be notified.If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, RAD will also inform those individuals without undue delay.

RAD will keep a record of any personal data breaches, regardless of whether it is required to notify.

Appendix A –Data Protection Practice Responsibilities

Keep data security at the heart of everything you do

- Clear your desk of any personal data when left unattended.
- Lock your computer when unattended (Use control, alt, delete to bring up lock option)
- Ensure your work mobile phone can only be unlocked by a passcode or fingerprint
- Put any personal data away when you leave the office
- Ensure that personal data is securely stored in a lockable filing cabinet and that all filing cabinets are locked every night.
- Personal data that is being taken out of the office should be treated with the utmost of care and security.
- Don't leave laptops, work mobile phones or personal data in your car overnight
- Don't put personal data on unencrypted memory sticks
- Keep passwords secure and change regularly. Do not disclose passwords to anyone without consent from your line manager
- Dispose of any paper waste containing personal information securely by shredding.
- Prevent virus attacks by taking care when opening emails and attachments or visiting new websites.
- Visitors should be signed in and out of the premises and accompanied in areas normally restricted to staff.
- Position computer screens away from windows to prevent accidental disclosures of personal data.
- Protect personal or confidential data sent electronically with a password with a minimum of 8 characters

Privacy notices

Remember the privacy notice for your project describes how we can use that personal data. We should not use that personal data in any other way without updating the privacy notice. We will need to let people know if we make material changes to our privacy notices. Each member of staff is responsible for ensuring that personal data is used and stored as described for their project in the relevant privacy notice and highlighting where changes need to be made to RAD's senior management team.

Appendix B – Subject Access Request Procedure

Introduction

Individuals have the right to access their personal data. This is commonly referred to as subject access. Individuals can make a subject access request verbally or in writing. **It can also be made to any part of RAD (including by social media) and does not have to be to a specific person or contact point.** RAD have one month to respond to a request. However where we have any uncertainty about the identity of the person making the request we will ask for more information to confirm identity. The period for responding to the request begins when RAD receives the additional information for identification. Please note that we cannot charge a fee to deal with a request in most circumstances. However, where the request is manifestly unfounded or excessive RAD may charge a "reasonable fee" for the administrative costs of complying with the request. This will be determined by the CEO. We have the right to refuse a subject access request where data is requested at unreasonable intervals, manifestly unfounded or excessive. You will be notified of the reasons as soon as possible.

Process

1. Request is received – if in writing pass immediately to CEO, if verbal take down details using form below and then pass to the CEO immediately. The CEO will determine if there is sufficient information to comply with the request.
2. Where necessary, inform person making request as soon as possible that we will need more information before responding to their request. Where information is needed to confirm identity, the Information may posted or brought into RAD by prior arrangement. However we will inform the individual that if they decide to post original identifcation it must be sent by recorded / registered delivery as RAD cannot be held responsible for items lost in the post. Proof of identity can be two from a recent utility bill, bank statement, passport or driving licence.
3. The CEO will coordinate the response within one month of confirming identity. In addition to a copy of the requested personal data, RAD will also provide individuals with the following information where relevant, much of which will already have been provided in our relevant privacy notice.):
    - the purposes of RAD's processing;
    - the categories of personal data concerned;
    - the recipients or categories of recipient RAD discloses the personal data to;
    - RAD's retention period for storing the personal data or, where this is not possible, the criteria for determining how long RAD will store it;
    - the existence of their right to request rectification, erasure or restriction or to object to such processing;
    - the right to lodge a complaint with the ICO or another supervisory authority;
    - information about the source of the data, where it was not obtained directly from the individual;
    - the existence of automated decision-making (including profiling); and
    - the safeguards you provide if you transfer personal data to a third country or international organisation.

Information required for Subject Acccess Request

1. Personal details

Surname:	Former surname (if applicable):
Title:	First name:
Date of birth:	
Present address:	Postcode:
Phone number:	Mobile number:
Email address:	

If you have lived at the above address for less than two years

Previous address:	Postcode:

2. Details of the information you require

Please give as much information as you can about particular areas to search so that we can give you what you require. Continue on a separate sheet if necessary.

Appendix C – Data breach procedure

Introduction

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. This includes breaches that are the result of both accidental and deliberate causes, for example, if you mislay any paperwork, files or electronic device containing personal data, or if you suspect that our security may have been breached in some way. RAD must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. Significant fines can be made if RAD does not report a breach when required to do so.

Process

1. You become aware of or suspect any data breach or a security incident occurs (such as a break in).
2. Contact the CEO immediately providing as much detail about the incident as possible.
3. The person discovering the breach will record all details of the incident in writing as soon as possible.
4. The CEO will determine whether a breach has occurred, whether this should be reported to the ICO and whether affected individuals need to be informed.
5. The CEO will coordinate actions to contact affected individuals where this has been deemed necessary with the following information:
    - the name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained;
    - a description of the likely consequences of the personal data breach; and
    - a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.
6. If the breach is notifiable to the ICO the CEO will report this breach to the ICO as soon as possible or within 72 hours, even if all details aren't currently known. If this is not possible reasons must be given for the delay.
7. The Chair of Trustees will be informed of the breach.
8. The CEO will coordinate an investigation of whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.
9. Details of the breach and its investigation will be recorded on the RAD system and reported to the Trustee Board.

REMEMBER YOU MUST REPORT ANY SUSPECTED DATA BREACH TO THE RAD CEO IMMEDIATELY ON BECOMING AWARE OF IT.