Data Protection Policy

Contents

Purpose of the policy

The purpose of data protection legislation and policies is to protect individuals from unauthorised disclosure of personal information.

RAK is subject to the Data Protection Act 2018 ~~1998~~ which came into force on 25 May 2018 ~~1 March 2000~~ and incorporates the EU ~~and the~~ General Data Protection Regulations (GDPR) ~~which came into force on 25 May 2018~~ because it holds **personal data** relating to clients, volunteers, staff, trustees, supporters and contacts. We owe a duty of confidentiality to our clients and we also wish to protect our own information.

RAK provides services to people from refugee backgrounds. In the course of this work, staff and volunteers frequently receive personal (and often sensitive) information about clients. The data ranges from basic information such as names, addresses, e-mail addresses and telephone numbers to **sensitive personal data,** particularly about clients and volunteers. **Sensitive personal data** may include details, such as physical and mental health, which are required to enable RAK to meet its charitable objectives – for example advice or counselling service or provision of confidential support.

The information RAK uses exists in many forms: printed or written paper, stored electronically, transmitted by post or sent by fax or electronically.

RAK is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data. This includes

RAK clients, as well as staff, volunteers, trustees and RAK supporters and contacts.

RAK will therefore follow procedures which aim to ensure that everyone who is authorised to access RAK systems and/or information, all employees and volunteers, and others who have access to any personal data held by or on behalf of the organisation, are fully aware of and abide by their duties under the Data Protection Act 2018 and the GDPR as it applies in the UK ~~2018~~.

1] Statement of policy

All personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act and Regulations to ensure this.

Given the nature of RAK services and its aims and principles, we view the lawful and correct treatment of personal information as very important to its successful operations, and to maintaining confidence between the organisation and those with whom we carry out business or provide services to.

To this end, RAK fully endorses and adheres to the principles of data protection as set out in the Data Protection Act 2018 and the GDPR ~~2018~~.

2] The principles of data protection

RAK will comply with the principles ~~of good practice~~ set out in the Data Protection Act 2018 Part 3 Chapter 2 ~~Schedule 1 Part 1 and Schedule 3, as amended by the GDPR which are legally enforceable~~. (See appendix 1.)

RAK will also follow the conditions for the processing of any personal data and will make a distinction between personal data and “sensitive” personal data as defined by the Act and set out in Schedule 2. (See appendix 2.)

In order to comply with the legislative requirements, RAK will:

a. have legitimate grounds for collecting and using the personal data;
b. not use the data in ways that have unjustified adverse effects on the individuals concerned;

c. be transparent about how the data will be used, and give individuals appropriate privacy notices when collecting their personal data.

d. handle people's personal data only in ways they would reasonably expect; and

e. endeavour to ensure that nothing unlawful is done with the data.

3] Handling of personal / sensitive information

a) Through appropriate management and the use of strict criteria and controls RAK will:

- observe conditions regarding the fair collection and use of personal information.
- meet its legal obligations to specify the purpose for which information is used.
- collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- to ensure consent is freely given, privacy notices will be in clear and plain language and printed on our new client registration form and new volunteer application form. We will seek separate permission from existing clients and volunteers who registered or applied before 25 May 2018 to communicate by email or text/telephone where there is no legitimate interest as a basis for processing e.g. invitations to social events, fundraising requests.
- where we are instructed directly by a child (under 18) to act for them RAK will take particular care to explain their rights under the Data Protection legislation and where possible obtain parental consent or consent from a person with parental responsibilities.
- ensure the quality of information used.
- ensure that processes are in place to help keep the data up to date.
- apply checks to ensure that file records are kept for six complete years, and then destroyed in accordance with the Data Protection Act, unless we can demonstrate a need to hold the data for longer.
- take appropriate technical and organisational security measures to safeguard personal information.
- ensure that personal information is not transferred abroad without suitable safeguards.

- ensure that the rights of people about whom the information is held can be fully exercised under the Act.

b) These rights include:

- The right to be informed that processing is being undertaken
- The right of access to one's personal information within the statutory 28 days
- The right to prevent processing in certain circumstances
- The right to correct, rectify, block or erase information regarded as wrong information
- The right to have incomplete data completed
- The right to erase information, unless there is a good reason to retain it
- The right to have the data transferred directly to another named party
- The right to complain to a supervisory authority e.g. the Information Commissioner and have the complaint investigated
- The right to take action against RAK if it is not complying with its Data Protection responsibilities and claim for damages

c) In addition, we will ensure that:

- The RAK Trustees and the Director are ultimately responsible for data protection, data quality and information security at RAK
- Everyone managing and handling personal information at RAK understands that they are individually and contractually responsible for following RAK policies and guidance and good data protection practice
- Everyone managing and handling personal information is appropriately trained to do so
- Everyone managing and handling personal information is appropriately supervised
- Any member of staff or volunteer or a member of the public who seeks to obtain information understands the procedure
- Queries about handling personal information are promptly and courteously dealt with
- Methods of handling personal information are regularly assessed and evaluated
- Performance with handling personal information is regularly assessed and evaluated

- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

d) All employees and volunteers at RAK will be made fully aware of this policy and of their duties and responsibilities, and will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. In particular they will ensure that:

- Paper files and other records or documents containing personal / sensitive data are kept in a secure environment
- Personal data held on computers and computer systems is protected by the use of secure passwords
- Individual passwords are such that they are not easily compromised.

4] Use of Case Management System

RAK uses Lamplight Database Systems Limited to electronically record the advice given to clients.

Lamplight facilitates adherence to the Data Protection Act and GDPR as it has a 'check box' to allow RAK to enter the fact that consent has been obtained. This 'check box' can be updated on every contact.

The servers (for data storage and application access) are provided by AWS in secure facilities: AWS is certified ISO27001:2013. Lamplight and AWS ensure that RAK data is stored in a secure environment.

5] Implementation

The Director is responsible for leading and monitoring policy implementation. s/he will also have overall responsibility for:

- the provision of cascade data protection training for staff and volunteers within the organisation
- carrying out compliance checks throughout the organisation to ensure adherence with the Data Protection Act and GDPR.

In the case of a breach of personal data, we may need to notify the applicable regulatory body and the individual.

a) If you know or suspect that a personal data breach has occurred, inform the director immediately. You should preserve all evidence relating to a potential personal data breach.

Dealing with subject access requests

a) Individuals may make a formal request for information we hold about them. Anyone who receives such a request should forward it to the director (director@refugeeactionkingston.org.uk) immediately. Nobody should feel bullied or pressured into disclosing personal information.
b) When receiving telephone enquiries, we will only disclose personal data if we have checked the caller's identity to make sure they are entitled to it.

6] Relationship with existing policies and supporting documentation

This policy has been formulated within the context of the RAK Confidentiality Policy, Keeping Information Secure Guidance, Client Registration Form, Client Care Letter, Authorisation Form and Volunteer application form.

7] Document History

Version 1 Reviewed July 2016

Version 2 Revised May 2018

Appendix 1

~~Schedule 1 to the~~ Part 2 Chapter 35 of the Data Protection Act 2018 lists the data protection principles as summarised in the following terms: ~~Points 6 and 8 are now covered elsewhere in the GDPR.~~

1. The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

~~Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –~~

~~(a) at least one of the conditions in Schedule 2 is met, and~~

~~(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.~~

2. The second data protection principle is that –

(a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and

(b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

~~Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes~~.

3. The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed. ~~Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed~~.

4. The fourth data protection principle is that -~~Personal data shall be accurate and, where necessary, kept up to date~~.

(a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and

(b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

5. The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed. ~~Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes~~.

6. The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures. ~~Personal data shall be processed in accordance with the rights of data subjects under this Act~~.

~~7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.~~

~~8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.~~

Appendix 2

Glossary

“Processing” broadly means collecting, using, disclosing, retaining or disposing of personal data, and if any aspect of processing is unfair, there will be a breach of the first data protection principle – even if you can show that you have met one or more of the conditions for processing.

Identification of Personal and Sensitive Data

Can a living individual be identified from the data, or, from the data and other information in your possession, or likely to come into your possession?

Does the data ‘relate to’ the identifiable living individual, whether in personal or family life, business or profession?
Is the data ‘obviously about’ a particular individual?
Is the data ‘linked to’ an individual so that it provides particular information about that individual?
Is the data used, or is it to be used, to inform or influence actions or decisions affecting an identifiable individual?
Does the data have any biographical significance in relation to the individual?
Does the data focus or concentrate on the individual as its central theme rather than on some other person, or some object, transaction or event?
Does the data impact or have the potential to impact on an individual, whether in a personal, family, business or professional capacity?

Sensitive personal data means personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal

Reviewed May 2018