

Data Protection Policy

1. Definitions

- 1.1. In this document 'Read Easy UK' means the registered CIO (charitable incorporated organisation) which acts as the umbrella body for Read Easy's volunteer groups. (charity number 1151288)
- 1.2. 'Affiliated Groups' means the volunteer-led groups that have affiliated to Read Easy UK.
- 1.3. Where the expression "Read Easy" or "the organisation" is used, it means the CIO and/or those persons who comprise each Affiliated Group from time to time.
- 1.4. **Data** is information that is stored electronically, on a computer, or in certain paper-based filing systems.
- 1.5. **Data Subjects** include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data. For the purpose of this policy, includes all Volunteers, Readers and any other individual for whom the Organisations hold Personal Data
- 1.6. **Data Controllers** are the people who, or organisations which, determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Law.. In relation to Affiliated Groups, the Data Controllers are the Management Team Members.
- 1.7. The **Data Protection Champion** is the day-to-day contact who deals with data protection queries for the local group. Each Affiliated Group must nominate a member of the Management Team to be its Data Protection Champion.
- 1.8. The **Data Protection Manager** is the person who has ultimate responsibility for ensuring that effective policies, procedures, and training programs regarding privacy and data protection are adhered to across Read Easy UK. Our Data Protection Manager is Faye Padfield (Head of Administration and Finance), is located in the United Kingdom (the "UK") and can be contacted at info@readeasy.co.uk regarding this data protection policy.
- 1.9. **Data Processors** include any third party that processes Personal Data on behalf of, or on the instructions of Read Easy UK or an Affiliated Group. This could be an IT services company, a fund raiser or a data shredding company.
- 1.10. **Data Users** include specific persons within the Organisations whose work involves using Personal Data. Data Users have a duty to protect the information they handle in accordance with this Data Protection Policy at all times. In the case of Affiliated Groups, data users will be Volunteers including members of the Management Team.
- 1.11. **Personal Data** means data relating to living individual, whether a Volunteer, an Employee, a Donor/Funder or a Reader who can be identified from that data (or from that data and other information in our possession). For the purpose of this policy, personal data can be factual and includes, but is not limited to a person's name;



address; email address telephone number; references obtained through the recruitment process or to one or more factors specific to the physical, physiological, mental, economic or cultural identity of that person etc. Personal Data may also be photographs, or an opinion about that person, their actions and behaviour.

- 1.12. **Processing** means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing may also include transferring personal data to third parties.
- 1.13. **Special Categories of Personal Data** (may also be referred to as Sensitive Personal Data) includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Special Categories of Personal Data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.
- 1.14. **Pseudonymisation** may involve replacing names or other identifiers which are easily attributed to individuals with, for example, a reference number.
- 1.15. **Encryption** a method by which information is converted into secret code that hides the information's true meaning.
- 1.16. **ICO** means the Information Commissioners Office, the UK regulator of the Data Protection Act.

2. Policy statement

- 2.1. Read Easy is a “data controller” for the purposes of the Data Protection Act 2018 and the retained EU law version of the General Data Protection Regulation (EU) 2016/679 (the “Law”). We have a legal obligation to comply with the Law when keeping personal data about third parties in a computer or in certain filing systems and when we obtain, use, disclose or otherwise process such data. As part of our obligations, we have a responsibility to protect any personal data we hold.
- 2.2. Everyone has rights under the Law with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our volunteers, Readers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in our organisation and enable us to operate successfully.
- 2.3. Failure to meet our responsibilities and obligations under the Law, including failures to notify the ICO or Data Subjects (as required), may expose Read Easy to regulatory sanctions, corrective measures, or other liabilities. Such liability may include, but is not limited to, formal investigations from the ICO and administrative fines of up to €10 million or 2 *per cent* of global turnover (whichever is the greater).
- 2.4. This policy sets out the basis on which we will process any personal data we collect from individuals, that is provided to us by the individuals themselves or other sources.



- 2.5. This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

3. To whom does this policy apply?

- 3.1. This policy applies to all Employees, Volunteers and Contractors of the charity and all Personnel retained by us from time to time (together our “**personnel**”), in addition to all Volunteers and Readers of each Affiliated Group (each a “**data subject**”).
- 3.2. Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

4. Processing Personal Data

- 4.1. The types of personal data we may be required to handle include information about our current, past and prospective Readers and other third parties that we communicate with (e.g. suppliers). The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Law.
- 4.2. Anyone processing personal data must ensure that personal data is
- 4.2.1. processed fairly, transparently and lawfully;
 - 4.2.2. collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes.
 - 4.2.3. adequate, relevant and limited to what is necessary in relation to the purpose accurate and kept up to date, either rectifying or erasing inaccurate personal data not kept in a form that can identify the data subject for longer than necessary for the purpose for which it is processed; and
 - 4.2.4. processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing, against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- 4.3. Each Organisation is responsible and accountable for ensuring compliance with the data protection principles noted above.

5. Lawful processing

- 5.1. The Law is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.
- 5.2. For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Law. These include, among other things, the data subject’s consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.
- 5.3. We will only collect personal data to the extent that it is required for the specific purpose



notified to the data subject.

- 5.4. The documents Read Easy UK has developed for use by Affiliated Groups reflect the level of personal data we feel it is appropriate to collect.

6. Notifying data subjects

- 6.1. If we collect personal data directly from data subjects, we will inform them about:
- 6.1.1. our identity and contact details and those of our Data Protection Manager;
 - 6.1.2. the purpose for and legal basis on which we intend to process their personal data, including any legitimate interests pursued by us;
 - 6.1.3. the types of third parties, if any, with which we will share or to which we will disclose that personal data;
 - 6.1.4. any transfer of personal data to a third country or international organisation, along with whether the country or countries in question have been found to have an adequate level of protection and the security measures that are in place to protect their personal data (if applicable);
 - 6.1.5. the period for which the personal data will be stored or the criteria used to determine this period;
 - 6.1.6. how data subjects can object to or limit our use and disclosure of their personal data;
 - 6.1.7. whether there is a legal or contractual requirement or obligation to provide personal data and the possible consequences of not doing so;
 - 6.1.8. any existence of automated decision making or profiling including the significance and consequences of processing personal data in this way; and
 - 6.1.9. the existence of a data subject's rights as outlined below.
 - 6.1.10. If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

7. Processing in line with a data subject's rights

- 7.1. We will process all personal data in line with data subjects' rights and we will inform data subjects of their right to:
- 7.1.1. be informed about the personal data we collect about them;
 - 7.1.2. obtain confirmation from us that their personal data is being collected and used by us;
 - 7.1.3. request access to any data held about them by us;
 - 7.1.4. prevent the processing of their data for direct-marketing purposes or a legitimate interest or the performance of a task in the public interest;
 - 7.1.5. ask to have inaccurate data amended;
 - 7.1.6. ask to have their personal data deleted or removed at any time;



7.1.7. block or stop us from collecting their personal data;

7.1.8. prevent processing that is likely to cause damage or distress to themselves or anyone else; and

7.1.9. obtain and reuse any personal data we hold about them for their own purposes.

7.2. To make any requests as listed above, data subjects should contact the Data Protection Champion at their Affiliated Group in the first instance, or the REUK Data Protection Manager via info@readeasy.org.uk should the Group no longer exist.

7.3. We will confirm any requests relating to the rights above within one month of receipt of a request from a data subject, or within two months of receipt of a request where this request is more complex.

8. Accurate personal data

8.1. The following procedures should be followed to ensure that all personal data kept is accurate and up-to-date:

8.2. Any inaccuracy in Personal Data should be brought to the attention of the Organisation's Coordinator or Management Team as soon as possible. It will then be the responsibility of the Data Protection Champion to correct the inaccuracy.

8.3. All Volunteers should notify their group's Team Leader, and Readers should notify their group's Coordinator as soon as possible of any change of their personal details. The Organisation concerned will then be able to contact them in future or, in the case of an emergency, contact another designated person.

8.4. Team Leaders should also notify their Regional Adviser as soon as possible of any changes to their personal details.

8.5. Employees should notify the Head of Administration and Finance as soon as possible of any change of their personal details.

8.6. Each group's Data Protection Champion will be responsible for ensuring that a yearly audit is carried out of all personal data held in both manual or computerised records to ensure the data held is accurate and up to date. A suitable Data Protection Annual Audit sheet is provided as an Appendix (G) to this policy.

9. Retention of personal data

9.1. We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

9.2. The Data Retention Schedule below provides an overview of the most common types of data Read Easy UK and/or Affiliated Groups are likely to hold. This reflects legal advice Read Easy UK has received as to the potential legal liability of each Organisation. This is a non-exhaustive list and groups should ensure they are aware of all personal data they hold, and where/by whom it is held. A copy of the items from the table below, specifically relevant to Affiliated Groups is also available a separate document in Appendix H to this policy.



Examples of data Read Easy routinely holds	Purpose(s) of collection/processing and storage	Category Type(s) of data	Lawful basis	Data retention period
Personal Data of Readers, Coaches and Management Team members, however received e.g. via website or paper forms, email, referral letter etc. (Includes personal data of any third parties such as referrers, emergency contacts and chaperones)	To register new Readers or Volunteers (e.g. personal details, emergency contacts, criminal convictions)	(a) Identity (b) Contact (c) Sensitive Personal Data	Necessary for our legitimate interests (to help people learn to read) Consent	7 years after the individuals stops reading/volunteering with us Disclosure forms received back from the Disclosure and Barring Service following an Enhanced DBS Check are NOT to be retained. The data subject's file is simply marked to indicate their suitability for working with the particular Reader assessed as "at risk" (necessitating the Enhanced DBS check). As per DBS check code of practice (Home Office)
Personal Data of unsuccessful Volunteer applicants, however received e.g. via website or paper forms, email, etc.	To recruit new Volunteers (e.g. personal details, emergency contacts, suitability for role)	(a) Identity (b) Contact (c) Sensitive Personal Data	Necessary for our legitimate interests (to help people learn to read) Consent	6 months after the conclusion of the recruitment process
Reading Record sheets Coordinator Coach and Reader monitoring records	To monitor the progress of our Reading Coach services	(a) Identity (b) Contact (c) Sensitive Personal Data	Necessary for our legitimate interests (to help people learn to read) Consent	Full length of period for which services are being used & then 6 months afterwards.
Reader/Volunteer stories, photographs or videos	To share good news and success stories	(a) Identity (b) Contact (c) Sensitive Personal Data	Necessary for our legitimate interests (to develop our charity and promote our cause) Consent	7 years after the individual stops reading/volunteering with us, unless express permission given for longer use



Examples of data Read Easy routinely holds	Purpose(s) of collection/processing and storage	Category Type(s) of data	Lawful basis	Data retention period
Minutes of all team meetings	To ensure good governance and management Potential future insurance claims	(a) Identity (b) Contact (c) Sensitive Personal Data	Necessary for our legitimate interests (to help people learn to read) Public task	7 years
Safeguarding records	To safeguard adults 'at risk' Potential future insurance claims	(a) Identity (b) Contact (c) Sensitive Personal Data	Legal Obligation	7 years after the individual stops reading/coaching with us
Financial data e.g. bank account/ credit card statements, expense claim forms, invoices; gift aid claims,	To ensure financial probity and security	(a) Identity (b) Contact (c) Financial (d) Transaction	Necessary for our legitimate interests (to help people learn to read) Necessary to comply with a legal obligation	7 years
Donation letters/receipts	To receive donations (e.g. personal details, contact details, gift aid declarations).	(a) Identity (b) Contact (c) Financial (d) Transaction	Necessary for our legitimate interests (to help people learn to read)	7 years after we receive the donation
Personal data such as name and contact details or "mailing lists" for newsletters or other direct communications to Readers, Volunteers, Donors/Funders, or Supporters – whether electronic or paper based	To manage relationships which will include: (a) Notifying people about changes to our terms or Privacy Notice; (b) Asking to leave a review or take a survey; and (c) Responding to a message or communication. To contact relevant parties about use of our programs, services, products, activities, special events, or other news that may be of interest to you and for otherwise marketing our services.	(a) Identity (b) Contact (c) Communication	Necessary for our legitimate interests (to develop our charity and promote our cause)	2 years after last contact with us



Examples of data Read Easy routinely holds	Purpose(s) of collection/processing and storage	Category Type(s) of data	Lawful basis	Data retention period
Data collected through our website	To administer and protect our charity and our website (including troubleshooting, data analysis, testing system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	Necessary for our legitimate interests (for running our charity, provision of administration and IT services, network security and to prevent fraud) Necessary to comply with a legal obligation	2 years after the data is collected for this purpose
Data collected through our website	To use data analytics to improve our website.	Technical	Necessary for our legitimate interests (for running our charity, provision of administration and IT services, network security and to prevent fraud) Necessary to comply with a legal obligation	2 years after the data is collected for this purpose
Data collected through our website	To use data analytics to improve our website.	Communication	Necessary for our legitimate interests (to develop our charity and promote our cause)	2 years after the data is collected for this purpose

- 9.3. Should an Affiliated Group close, the Management Team should ensure that the information listed above is retained and securely stored in line with the above retention periods, and that Read Easy UK is informed of its whereabouts. Alternatively, Read Easy UK can store this information as a service to the Affiliated Group.

10. Data security

- 10.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, we will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.



- 10.2. We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he or she agrees to comply with those procedures and policies, or if he or she puts in place adequate measures themselves.
- 10.3. We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:
 - 10.3.1. Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored in either the relevant Affiliated Group's SharePoint site or One Drive, or the individual user's One Drive using their Read Easy log in, instead of individual PCs.
 - 10.3.2. Confidentiality means that only people who are authorised to use the data can access it. Personal data that is stored electronically in shared areas as detailed in 10.3.1 should be either password protected or access permissions only given to those who need to use it as part of their role.
 - 10.3.3. Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- 10.4. Security procedures include:
 - 10.4.1. **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal data is always considered confidential.)
 - 10.4.2. **Methods of disposal.** Paper documents should be shredded. Digital storage devices e.g. memory sticks should have data erased or should be physically destroyed when they are no longer required. If computers that contain personal data are to be disposed of, personal data must be deleted beforehand. Where applicable, a Volunteer or Employee who ceases work with the Organisations will be asked to hand over any personal data that they hold to the Organisations.
 - 10.4.3. **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended. Computers or other devices, such as laptops, memory sticks, CDs etc. that hold Personal Data should be password protected.
 - 10.4.4. The **pseudonymisation** and **encryption** (see definitions in Section 1) of personal data where appropriate.
- 10.5. Further information for Affiliated Groups and their Volunteers on keeping data secure is provided in Appendix F.
- 10.6. In addition to the above, the security procedures that Read Easy UK will implement for all Organisations include:
 - 10.6.1. Ensuring ongoing confidentiality, integrity, availability and resilience of Read Easy UK processing systems and services.
 - 10.6.2. Ensuring we can restore access to personal data held on Read Easy UK



systems in a timely manner if a physical or technical incident occurs.

- 10.6.3. Regular testing, assessment and evaluation of the effectiveness of our technical and organisational measures to ensure personal data is secure.

11. Dealing with subject access requests (SAR)

- 11.1. All Volunteers, Employees and Readers have the right to access personal data held about them by the Organisations. When exercising this right, this is known as a Subject Access Request or SAR. All such requests should be forwarded to the relevant Data Protection Champion.
 - 11.1.1. Where possible, such requests should be made in writing. For Readers for whom this is not possible, the Data Protection Champion will write the details of the request on the behalf of the Reader, read this out to the Reader and obtain their signature, before providing the information. They should then provide the Reader with a copy of this signed request.
 - 11.1.2. Information will be gathered from all relevant filing systems and computerised records and supplied in hard copy to the individual.
 - 11.1.3. The information supplied should also include an explanation of any codes or terms used.
 - 11.1.4. Organisations must comply with SAR without undue delay and at the latest within one month of receiving the request. You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual, e.g. other types of requests relating to individuals' rights.

12. Dealing with a breach, or suspected breach of data

- 12.1. Most personal data breaches can be categorised according to the following security principles:
 - 12.1.1. "Confidentiality Breaches," where there is an unauthorised or accidental disclosure of, or access to, Personal Data;
 - 12.1.2. "Integrity Breaches," where there is an unauthorised or accidental alteration of Personal Data; or
 - 12.1.3. "Availability Breaches," where this is an accidental or unauthorised loss of access to, or destruction of, Personal Data.
 - 12.1.4. Personal Data Breaches may occur in a number of ways, for example:
 - 12.1.5. loss or theft of data or equipment on which data is stored, for example the loss of a laptop or paper files;
 - 12.1.6. inappropriate access controls allowing unauthorised use;
 - 12.1.7. equipment failure;
 - 12.1.8. human error, such as sending an email to the wrong recipient;
 - 12.1.9. unforeseen natural events such as a fire or flood; and



12.1.10. hacking, phishing and other attacks where information is obtained by deception.

- 12.2. If you become aware of or suspect any possible or actual Personal Data Breach it is critical that you notify your group's Data Protection Champion immediately, or the Read Easy UK Data Protection Manager, Faye Padfield via info@readeasy.org.uk.
- 12.3. Individuals other than the nominated Data Protection Champion and Manager must not take any further action in relation to the breach. In particular, they must not notify any affected individuals, regulators or members of the media. The Data Protection Champion or Read Easy UK will acknowledge receipt of the disclosure (if the person making the report has given their name) and take the appropriate steps to deal with the report.

13. Disclosure of information to third parties

- 13.1. The Organisations aim to keep personal data within their control. The Organisations will only provide personal data that is strictly necessary to ensure the health and safety of Volunteers, Employees and Readers.

14. Providing information over the telephone

- 14.1. Any volunteer or member of staff dealing with telephone or email enquiries should be careful not to disclose any personal data about others without their express consent. In particular, they should:
 - 14.1.1. Check the caller's identity to make sure that information is only given to a person who is entitled to it.
 - 14.1.2. Suggest that the caller put their request in writing if the volunteer or employee is unsure about the caller's identity and where their identity cannot be checked.
 - 14.1.3. Refer to the Coordinator or the Data Protection Champion for assistance in difficult situations. No-one should feel pressured or bullied into disclosing Personal Data.

15. Registration with the ICO

- 15.1. Under the Data Protection Act 2018, which incorporates UK GDPR, Organisations which are established for not-for-profit making purposes can be exempt from registration with the ICO.
- 15.2. The exemption only applies to processing if:
 - 15.2.1. you only process information necessary to establish or maintain membership or support;
 - 15.2.2. only process information necessary to provide or administer activities for people who are members of the organisation or have regular contact with it; This would include giving support to individuals. It is also clear that although the contact the organisation has with people should be regular, it does not need to be frequent. So an organisation that provides activities or support on an ongoing basis to the same individuals (even if a minority only contact the organisation once) will fall within the exemption;
 - 15.2.3. you only hold information about individuals whose data you need to process for



this exempt purpose;

15.2.4. the personal data you process is restricted to personal information that is necessary for this exempt purpose.

- 15.3. Read Easy UK therefore expects that Affiliated Groups will be exempt from the legal requirement to register with the ICO. However, Data Protection Champions are encouraged to carry out a self assessment with the ICO for their Affiliated Group to ensure their group meets the requirements of this exemption: [Registration self-assessment | ICO](#)
- 15.4. Affiliated Groups may still choose to voluntarily register with the ICO, and this is a relatively simple process which takes around 15 minutes online: [ICO - Pay your data protection fee](#). The annual fee is currently £40 for charity registration (2021).
- 15.5. Regardless of whether Affiliated groups register with the ICO or not, all Organisations are required to adhere to the principles of the UK GDPR and understand best practice for managing information. This can be best achieved by Affiliated Groups by following the procedures and guidance set out in this Read Easy UK Data Protection Policy and its appendices.

16. Note about Privacy Notices and Appendices

- 16.1. Please note that Data Protection regulations requires all individuals whose data we process to be notified about their rights with regard to data protection. In order to help Affiliated Groups to meet this requirement, Read Easy UK has made available Privacy Notices specifically tailored for the various people whose data we may process in the course of our activities.
- 16.1.1. Appendix A - Privacy Notice for Volunteers. This is intended for all Volunteers who take up roles in the Organisations. It is also included in the relevant Volunteer Handbooks. (A shorter version for potential Volunteers is listed as Appendix D and is included in all Volunteer application forms)
- 16.1.2. Appendix B - Privacy Notice for Readers. Both a summary paragraph of this and the full appendix is included in the Reader Enrolment paperwork.
- The short summary paragraph must be read to all new Readers at enrolment and this is clearly indicated. This is not referenced as an appendix to avoid use of confusing language for new Readers.
- The full Privacy Notice for Readers in the Reader Enrolment Paperwork must be edited by each group to include the details of the Data Protection Champion, and a copy given to each Reader at enrolment.
- 16.1.3. Appendix C - Privacy Notice for Supporters and Donors is included as Appendix C to this policy and as an attachment to the Read Easy Fundraiser's Information Pack. This notice should be sent to all those who donate to the Organisations.
- 16.1.4. Appendix D – Summary Privacy Notice for Potential Volunteers. This is included at the bottom of all volunteer application forms, and separately as Appendix D to this policy.



- 16.1.5. Appendix E – This is Read Easy UK Website Privacy Notice, which is also available to download from each page of the Read Easy website.
- 16.2. Read Easy UK has also made the following provisions to assist Affiliated Groups to comply with their data protection regulations.
- 16.2.1. Appendix F: Keeping Data Secure – this is included in all Read Easy Handbooks as well as Appendix F to this policy. This provides general guidelines for data security and should be read and understood by all Volunteers, including Reading Coaches.
- 16.2.2. Appendix G: Data Protection Audit Sheet. This is provided to support each Data Protection Champion to carry out regular audits of all data held by their group.
- 16.2.3. Appendix H – Data Retention Schedule Table. This provides details of the types of data likely to be held, for what purpose and for how long each should be kept.
- 16.2.4. Appendix I: Dealing with a suspected, or actual, data breach. This provides details of the steps Data Protection Champion steps must take in the case of suspected or actual data breaches.
- 16.2.5. Appendix N: Photo and Publicity Form - this form can be used to gain explicit permission for using personal data such as name, story or photographs of Reader/Volunteers in publicity materials or online posts.
- 16.3. Please note Appendices J-M are used for forms specific to employees/associates and the Trustee Board of Read Easy UK.

It is the responsibility of the nominated Data Protection Champion of each Read Easy Affiliated Group to ensure that all involved with their group are provided with the necessary information.

17. Monitoring and review of the Policy

- 17.1. This policy is reviewed annually by Read Easy UK. Recommendations for any amendments should be reported via the Data Protection Champion of each Organisation.
- 17.2. We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.
- 17.3. Any breach of this policy will be taken seriously and may result in the Organisation concerned taking further action.

REUK Use Only

Author:	Read Easy UK/FP	
Title:	Data Protection Policy	
Status of policy:	Adopted by Trustees	
Date Published:	Nov 2021	Version: 1 (06/22)
Previous Version Date:	Sept 2019	
Next Review due:	Nov 2022	