

## DATA PROTECTION POLICY

### INTRODUCTION

- Reading Community Learning Centre (“RCLC” or “the Centre”) respects the private lives of individuals and recognises the importance of safeguarding personal privacy. RCLC appreciates the responsibility of storing personal data and considers the protection of personal data to always be a priority and a consideration throughout RCLC’s services.
- This policy provides guidance for all RCLC staff, trustees and volunteers and outlines considerations and management of personal data.
- Specific instructions for each block of information are detailed on a “data mapping sheet” and attached as appendices. A review of the management of personal data should be included within staff supervision meetings.
- Data Mapping Sheet (under Appendices) exist for the following areas. They are not part of the policy as they will be amended by the data controller as required. The current versions are attached for information.
  1. Staff
  2. Trustees and RCLC Members
  3. Volunteers (Active)
  4. Staff and Volunteer Applications (rejected or dormant)
  5. Learners
  6. Individual donors
  7. Referrers
  8. Contractors

### DEFINITIONS

- **Data subjects** are all the individuals whose personal data is being held or processed by RCLC. These could be staff, both paid and unpaid; learners, both prospective and current; supporters of the organisations; funders; and stakeholders.
- The **data controller** is the party who determines the purposes for which, and the manner in which, any personal data is used. In this case the data controller is RCLC, and the Trustees with the Centre staff are responsible for the implementation of this policy.
- The **designated data controller** is the person who will deal with day to day matters. RCLC has one designated data controller: the Centre Manager.
- The **data protection officer** is an appointed person who is competent in the principles of data protection and privacy, committed to the role and comfortable with raising difficult questions. The data protection officer must have the authority to challenge anyone at RCLC

and they cannot be fired or reprimanded for doing so. The RCLC data protection officer is the Centre Manager.

- **Personal data** is defined as “any information relating to an identified or identifiable natural person” and includes things like someone’s name, address, age, telephone number and hobbies.
- Some types of personal data are special categories of personal data or criminal convictions and offences data. These are considered to be more sensitive and you may only process them in limited circumstances. This includes racial or ethnic origin, political opinions and religious beliefs, physical or mental health, trade union membership and genetic or biometric data where it is used for the purpose of identifying someone (such as fingerprint access).
- There must always be a lawful basis for processing personal data. Consent is one form of lawful basis. You only need to include the types of lawful bases that you rely on. Most likely these will be consent, contract, and legitimate interests. This means that the collection and processing of data must be necessary for the performance of a contract, to comply with a legal obligation, to protect the data subject’s vital interests (such as the emergency services), or for the performance of a task in the public interest or in the exercise of official authority. The lawful basis can also be that the data is necessary for the purposes of the “legitimate interests” of the data controller or third party (note that any processing done under legitimate interests must be open to scrutiny of that justification and this designation should not be abused).

## I) TYPES OF DATA TO WHICH THIS POLICY APPLIES

The RCLC data protection policy applies to personal data, held under four areas:

1. Staff administration - appointments or dismissals, pay, discipline, superannuation, appraisals, work management and other personnel matters in relation to the staff of the Data Controller. Data subjects - staff both paid and unpaid. Volunteers and trustees are also included.
2. Fundraising and administration - fundraising in support of the objectives of the Centre. Data subjects - donors and lenders, prospective stakeholders and funding bodies.
3. Student database - information about all registered students.
4. Advice and information work - relating to anyone using the centre in a personal capacity. There is an advice log noting name, date and advice given.

## II) RESPONSIBILITY FOR DATA PROTECTION

1. As the data controller, RCLC is responsible for implementing this policy. The designated data controller will deal with the day-to-day matters of this.

2. The data controller will not collect personal data unless there is a lawful basis for doing so. If there is no legal basis, then personal data will not be collected without the consent of the data subject.
3. RCLC would disclose information *without consent* if it believes that:
  - a. a child is at risk of being harmed
  - b. a person's life or safety is at riskor:
  - c. if required by statute (e.g. there is a legal obligation to report drug trafficking/money laundering/terrorist activity to the police)
  - d. if required under a contractual obligation (e.g. where services are purchased by the local authority, etc, and that contract requires disclosure of certain information)
  - e. if required by a court or court order.

A disclosure of confidential information without permission would therefore be to the police, an authorised organisation (e.g. local authority) or to the courts.

### III) DATA COLLECTION

1. RCLC will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.
2. RCLC's use of any personal data will be grounded in a legal basis. If there is no legal basis, then RCLC will make sure that the data subject has consented to their information being used.
3. If required, consent given by the data subject in relation to their personal data will be:
  - a. Active - consent will be freely given and not enabled by default
  - b. Granular - the data subject will need to consent to each specific use of their data one at a time, rather than ticking one box to consent to multiple uses
  - c. Unbundled - the data subject will not have to give consent for one use of their data in order to give consent for any other use of their data
  - d. Named - the data subject will be made aware of all specific third parties who will be receiving their data and why they will be receiving it
  - e. Balanced - consent will not create an unfair relationship between the data subject and anyone using their data
  - f. Verifiable and documented - RCLC will be able to prove who gave their consent, how consent was given, what information they were given, what they agreed to, when they consented, and whether or not the user has withdrawn their consent.

4. When collecting data, RCLC will ensure that the data subject:
  - a. Clearly understands why the information is needed
  - b. Understands what it will be used for and what the consequences are should the data subject decide not to give consent to processing
  - c. Has given the appropriate consent for data to be processed
  - d. Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
  - e. Has received sufficient information on why their data is needed and how it will be used
  - f. Has received information that they can withdraw their consent at any time and how to do this.

#### IV) DATA STORAGE AND PROTECTION

##### 1. Storage

- a. All personal data, relating to both staff and learners, should be stored in a locked cupboard or on a password-protected computer.
- b. If a copy is kept on any kind of removable storage device, that device must itself be kept in a locked filing cabinet, drawer, or safe.
- c. All computer files are backed up daily on line.

##### 2. Protection

- a. All staff and trustees of RCLC are responsible for ensuring that any personal data that they hold is kept securely; personal data is not disclosed either orally, in writing, via web pages or by any other means, accidentally or otherwise, to any unauthorised third party, without the express permission of the data subject.
- b. The data shall be obtained for specific purposes and will not be used for any other purpose. RCLC will only use personal data for the purposes that the data subject has consented to.
- c. RCLC will make a reasonable effort to ensure the data obtained is accurate and will provide a method of regular review, in the Data Mapping Sheet, to keep it up to date as necessary.
- d. RCLC will not keep data for longer than is necessary. A review period will be specified in the Data Control Sheet and any data held that is no longer necessary will be deleted.
- e. RCLC will erase or restrict the processing of personal data held within a reasonable time or if requested by the individual.

- f. RCLC will take all measures to prevent unauthorised or unlawful processing of personal data and accidental loss or damage. The measures will be specified in the Data Control Sheet.
- g. RCLC will not transfer personal data outside the European Economic Area.

## V) DATA ACCESS AND ACCURACY

1. All data subjects have the following rights:
  - a. the right to access the information that RCLC holds about them
  - b. the right to be informed about the collection and use of personal data RCLC holds about them.
  - c. the right to have any inaccuracies in the data held about them corrected or completed if it is incomplete
  - d. the right to have their data erased when it is no longer needed for the purpose for which it was originally collected (also known as the 'right to be forgotten')
  - e. the right to object to having their data used for certain purposes
  - f. the right to obtain and reuse their data and take it to another service provider
  - g. the right to not be subjected to decision making based on automatic processing or profiling if this is not necessary under contract or under law.
  - h. the right to the restriction of the use of their data in certain circumstances, e.g. if some of their data is inaccurate.

RCLC will honour this right as necessary and as requested by data subjects. RCLC will take reasonable steps to ensure that data subjects' information is kept up to date by asking them whether there have been any changes.

2. In addition, RCLC will ensure that:
  - a. It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection - in this case it is the Centre Manager
  - b. Everyone processing personal data understands that they are contractually responsible for following good data protection practice
  - c. Everyone processing personal data is appropriately trained to do so
  - d. Everyone processing personal data is appropriately supervised
  - e. It deals promptly and courteously with any enquiries about handling personal data
  - f. It describes clearly how it handles personal data

- g. It will regularly review and audit the ways it hold, manage and use personal data
- h. 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. For volunteers this may result in RCLC applying the Volunteer Resolving Problems Procedure (please refer to RCLC Volunteer policy) and bringing their volunteering to an end.

## VI) ANTICIPATED RISKS

1. It is vital that all possible risks are identified by the Data Controller and the level of risk should be dictated by how the data is obtained and managed.
2. RCLC will ensure that suitable measures are taken under all circumstances to protect stored data. However there are anticipated risks which the charity might face. For example, there may be a small risk of an individual being subjected to direct marketing or a risk that an individual's faith, ethnicity, or sexual orientation etc is revealed by association and their home address identified by extremists.
3. In a situation of anticipated risk the data controller will take suitable action in agreement with the Board of RCLC.
4. The Board of RCLC has a risk register in place which addresses risks relating to data.
5. This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the UK General Data Protection Regulation ("UK GDPR").

In case of any queries or questions in relation to this policy please contact the RCLC Data Protection Officer, Aisha Malik.

Date Approved by Board: [Sep 2023](#)

Review Date [Sep 2026](#)

Signed on behalf of the Board of Trustees

---

Dated

---

**Appendix 1 Data Mapping Sheets**

Subject Type: Staff	Audit By: Aisha Malik	Date: 12/3/2023	Review Date: 20/6/2026
---------------------	-----------------------	-----------------	------------------------

**GDPR AUDIT-DATA MAPPING SHEETS**

Data held	Purpose of data	Responsibility for data	Where stored	Access permission	Retention period	How transmitted	Transmission destination	Existing security	Evidence of consent	Further measures required compliance	
Payroll (e.g. NI number, salary, bank account)	Payment/ Employment	AM	Locked filing cabinet in AM Office	AM	Ongoing and 6 years after leaving	Electronically	Payroll provider	Password for AM computer, antivirus, firewall,	Yes – new starter form	None	
HR records					SDT		By post	Pension Provider	Employment contract		
Pensions					LCE		Online password protected portal for Glasscubes	AM Pension folder, finance folder, HR Folders in locked, cabinet in a locked room	portal, pension portal, password for AM office		Tutor contract
Recruitment documentation (eg. CVs and Cover Letters)					Payroll office at David Jones and Co	Shaheen K	For BBO Project 11 years				Employment applications
Tutor contracts					B and C Holding (Pension Plus)	B and C Holding (Pension Plus)	Statutory maternity records 3 years from the end of leave				Signed contract
Teaching observations					AM Computer	Glasscubes BBO lead staff	Pension scheme 12 years from the end of any benefit payable	BBO Funding officer and project manager	Password protection Glasscubes		
					Back up data saved on online cloud Live drive on AM PC				Password for SDT computer, antivirus, firewall		
			Glasscubes (online portal BBO)		Sick pay records: 3 months after leave has been paid		Postage: use signed for delivery & LCE Computer password protected.				

GDPR AUDIT-DATA MAPPING SHEETS

Subject Type: Trustees and RCLC Members	Audit By: Aisha Malik	Date: 12/6/2023	Review Date: 12/6/2026
---	-----------------------	-----------------	------------------------

GDPR AUDIT-DATA MAPPING SHEETS

Data held	Purpose of data	Responsibility for data	Where stored	Access permission	Retention period	How transmitted	Transmission destination	Existing security	Evidence of consent	Further measures required to become compliant
Contact information (name, address, email, phone)  Background information (eg. Date of birth, DBS checks)  Recruitment documentation (eg. CVs and Cover Letters)  RCLC Membership records	Recruit trustees onto the board  Inform up date RCLC members on the work of RCLC and AGM notices	AM	Locked filing cabinet in AM Office  AM Computer  Back up data saved on online cloud Live drive on AM PC  SDT PC	AM  SDT	Ongoing and 6 years after leaving	Electronically  By Post	AM PC  SDT PC	Password for AM computer, antivirus, firewall, password for AM office  Password for SDT computer, antivirus, firewall	Declaration to Charity Commission and Companies House when registering and on application	None  Need to send out a GDPR notice letter to all members requesting if we can use their information to send RCLC update emails



GDPR AUDIT-DATA MAPPING SHEETS

Subject Type: Volunteers (active)	Audit By: Aisha Malik	Date: 12/6/2023	Review Date: 12/6/2026
-----------------------------------	-----------------------	-----------------	------------------------

Data held	Purpose of data	Responsibility for data	Where stored	Access permission	Retention period	How transmitted	Transmission destination	Existing security	Evidence of consent	Further measures required to become compliant
Contact information (name, address, email, phone)  Background information and Volunteer Application Form (eg. DBS Checks, references)	Recruit volunteers	AM & Shaheen K	Locked filing cabinet in AM Office  AM Computer  Back up data saved on online cloud Live drive on AM PC  Shaheen Kausar 'S PC and on the shared drive	AM  Shaheen Kausar	Ongoing and 6 years after leaving	Electronically  By post	AM PC  AM HR folders in lockable cabinet	Password for AM and Shaheen's computer, antivirus, firewall, password for AM office	Volunteer application form  Volunteer policy	None

GDPR AUDIT-DATA MAPPING SHEETS

Subject Type: Staff and Volunteer Applications (rejected or dormant)	Audit By: Aisha Malik	Date: 12/6/2023	Review Date: 12/6/2026
--	-----------------------	-----------------	------------------------

Data held	Purpose of data	Responsibility for data	Where stored	Access permission	Retention period	How transmitted	Transmission destination	Existing security	Evidence of consent	Further measures required to become compliant
Contact information (name, address, email, phone)  Background information and Volunteer Application Form (e.g. DBS Checks, references)	Recruit volunteers	AM	Locked filing cabinet in AM Office  AM Computer  Back up data saved on online cloud Live drive on AM PC  Shaheen Kausar 'S PC and on the shared drive	AM  SK	1 year	Electronically  By post	AM PC  AM HR folders in lockable cabinet	Password for AM &SK computer, antivirus, firewall, password for AM office	Signed application forms  Signed contracts	None

GDPR AUDIT-DATA MAPPING SHEETS

Subject Type: Learners	Audit By: Aisha Malik	Date: 12/6/2023	Review Date: 12/6/2026
------------------------	-----------------------	-----------------	------------------------

GDPR AUDIT-DATA MAPPING SHEETS

Data held	Purpose of data	Responsibility for data	Where stored	Access permission	Retention period	How transmitted	Transmission destination	Existing security	Evidence of consent	Further measures required for compliant
Enrolment forms and evidence of eligibility status, benefits, learner paperwork such as ILPs, registers and evaluations  Photos and film footage  Case studies  Children in the crèche-enrolment forms, registers and evaluations form	Requirement for funding  Data needed for fund raising, grant applications, research and monitoring of the charity's work, is it meeting its aims  RARPA  Contacting learners, monitoring equal opps and statistical purposes.	AM Shaheen K Administrator  Tutors (tel no for learners to contact them)	Teaching files  Paper based learner forms in the filing cabinet in admin office  Electronic database on AM PC, SK PC and shared drive and Live drive  Petra Robinson PC/ USB Stick-password protected  ND off site data storage BBO Glasscubes	AM SK Administrator PR Tutors  New Directions (DCLG Funding, BBO Funding, NLDC Funding)  RBC (SVPR Group)  BBO Project manager, ESF and BBO admin and monitoring team	Varies depending on the funder.  BBO Project: up to 10 years after the project ends: 2030  NLDC and controlling migration: 7 years	Copies of enrolments collected in person/ hand delivered to ND  Monitoring reports with summaries (not individuals) emailed electronically and sent in the post  BBO Glasscubes online portal electronic scanned data	AM office (locked filing cabinet)  SK and Admin office (filing cabinet)  Glasscubes portal data goes to BBO and ESF for monitoring	Password protection on all PCs, at RCLC, passwords to enter offices, computer, antivirus, firewall,  Password on Petra PC  ND adheres to GDPR  BBO Glasscubes GDPR compliant	Signed declaration on enrolment forms  Signed contracts  GDPR info sharing contract	None

Subject Type: Individual donors	Audit By: Aisha Malik	Date: 12/6/2023	Review Date: 12/6/2026
---------------------------------	-----------------------	-----------------	------------------------

**GDPR AUDIT-DATA MAPPING SHEETS**

Data held	Purpose of data	Responsibility for data	Where stored	Access permission	Retention period	How transmitted	Transmission destination	Existing security	Evidence of consent	Further measures
Name, address for HMRC Online donations  Just giving	To claim gift aid and raise funds for RCLC	AM	AM PC and Live Drive backup cloud  Just giving website  HMRC gateway for claiming gift aid	AM  HMRC	3 years	Electronically through the government gateway for HMRC	HMRC database	Password protection on am PC, passwords to enter offices, computer, antivirus, firewall  Government gateway password  Just giving password protected	Gift aid form filled in by donor	None

Subject Type: Referrers	Audit By: Aisha Malik	Date: 12/6/2023	Review Date: 12/6/2026
-------------------------	-----------------------	-----------------	------------------------

GDPR AUDIT-DATA MAPPING SHEETS

Data held	Purpose of data	Responsibility for data	Where stored	Access permission	Retention period	How transmitted	Transmission destination	Existing security	Evidence of consent	Further measures required to become compliant
Contact information (Name, work email, work phone, employer)	Refer clients who need to access RCLC services and also to refer RCLC clients onto partners	AM SK Tutors Admin staff	AM, SK and Admin PC and Live Drive backup cloud for AM PC  Tutor files in the tutor folder (this remains in a locked room)	AM SK Admin staff Tutors	Varies depending on the funders e.g. BBO Project: up to 10 years after the project ends: 2030  NLDC and controlling migration: 7 years	Referral form  Email exchange  Referral made over the phone in a conversation with the referrer	Organisation where learners is being referred to  RCLC (learners referred to RCLC)	Learners are part of the referral process-written declaration or are present at the time of the meeting for the referral.  Confidential data sharing  Password for AM computer, antivirus, firewall, payroll portal, pension portal, password for AM office	Enrolment forms  Referral forms  GDPR info sharing contract	None

Subject Type: Contractors	Audit By: Aisha Malik	Date: 12/6/2023	Review Date: 12/6/2026
---------------------------	-----------------------	-----------------	------------------------

**GDPR AUDIT-DATA MAPPING SHEETS**

Data held	Purpose of data	Responsibility for data	Where stored	Access permission	Retention period	How transmitted	Transmission destination	Existing security	Evidence of consent	Further measures required to become compliant
Signed contracts with service providers e.g. utilities, bank, payroll, pension, photocopiers etc	To keep a legal record of the services that are to be provided and received by RCLC	AM	AM locked filing cabinet in locked room  Head office of service providers  Live drive back up cloud of AM PC	AM  LCE	3 YEARS	Paper copies signed and posted between the two parties	One copy at RCLC- in AM locked cupboard and one copy at the service providers address  AM PC	Contracts kept in lockable cabinet in AM office which is password protected.  AM PC password protected  Password for AM computer, antivirus, firewall, payroll portal, pension portal, password for AM office	Signed contracts and GDPR info sharing contract	None