



Data Protection Policy & Guidelines

Policy prepared by:	Mike Farrington
Date:	13/10/2026
Signed:	
Policy review date:	13/10/2027
Version:	2.0

CONTENTS

	Page no.
1.0 INTRODUCTION	3
2.0 COMPLIANCE	3
3.0 DEFINITIONS	4
4.0 GENERAL DATA PROTECTION REGULATION	5
5.0 RESPONSIBILITIES UNDER THE GENERAL DATA PROTECTION REGULATION	6
6.0 DATA PROTECTION PRINCIPLES	6
7.0 INFORMATION SECURITY	7
8.0 DATA COLLECTION	8
9.0 DATA BREACH NOTIFICATION AND REPORTING	8
10.0 DATA SHARING	9
11.0 DATA STORAGE & RETENTION SCHEDULES	9
12.0 DISCLOSURE	10
13.0 SUBJECT ACCESS REQUESTS	10
14.0 CHILD PROTECTION AND DATA ACCESS	11
 ADDENDUM 1: COVID-19 AND DATA PROTECTION	 11

1.0 INTRODUCTION

1.1 Policy Statement

The Data Protection Act 2018 ('DPA 2018') protects the rights of individuals to have their personal data collected and stored securely and used only for legitimate and lawful purposes for which a valid legal basis exists. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) which became part of UK law from 25th May 2018. This policy sets out how Concrete Rose Collective CIC (Concrete Rose) complies with the General Data Protection Regulation.

Concrete Rose is committed to a policy of protecting the rights and privacy of individuals including employees, hosts, young people, business contacts, funders, volunteers and the other people the organisation has a relationship with or may need to contact, in accordance with the General Data Protection Regulation (GDPR). The new regulatory environment demands higher transparency and accountability in how organisations manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

1.2 Background

The GDPR contains provisions that Concrete Rose needs to be aware of as a data controller, including provisions intended to enhance the protection of individual's personal data.

Concrete Rose needs to collect and process certain information about employees, young people, business contacts, funders, supporters, volunteers and other people the organisation has a relationship with or may need to contact for various purposes such as, but not limited to:

- The recruitment and payment of staff
- The recruitment of volunteers and hosts
- The administration of our initiatives
- The provision of accommodation for young people (including contact and engagement with young people)
- Recording outcomes and evaluations of programme for external funding bodies
- Collecting fees
- Donations

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation, Concrete Rose must ensure that all this personal information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully. The reasons for this are to ensure that Concrete Rose:

- Complies with the law and principles of the Data Protection Act 2018 and the General Data Protection Regulation.
- Aims to maintain consistently high levels of best practice in processing of personal and/or sensitive data.
- Protects employees, programme participants and other individuals.
- Protects itself as an organisation.
- Is open about how it stores and processes individuals' data.

2.0 COMPLIANCE

2.1 Application

This policy applies to all staff and associates (hosts, volunteers etc) of Concrete Rose. Breach of this policy or of the Regulation itself will be considered an offence and will invoke disciplinary procedures. As a matter of best practice, other organisations and individuals working with Concrete Rose and who have access to

personal information, will be expected to read and comply with this policy. It is expected that all agreements (service level agreements, MoUs etc) with external bodies will include an agreement to abide by this policy.

This policy will be reviewed annually and updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

3.0 DEFINITIONS

3.1 Overview

The following list of definitions of the technical terms we have used is intended to aid understanding of this policy:

Data Controller – The person who (either alone or with others) decides what personal information Concrete Rose will hold and how it will be held or used.

Data Protection Act 2018 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

General Data Protection Regulation – Regulates the processing of personal data and protects the rights and privacy of all living individuals. This legislation provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that Concrete Rose follows its data protection policy and complies with the Data Protection Act 2018 and the General Data Protection Regulation 2016 (GDPR). The responsibility of the Data Protection Officer (DPO) is as follows:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed.

Data Subject – The individual whose personal information is being held or processed by Concrete Rose (for example: a young person, an employee, a volunteer, Organisation, Trust or a supporter).

Personal data – means data which relates to a living individual who can be identified –

- a) from the data or
- b) from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be “personal data”. The more expansive definition in the General Data Protection Regulation includes online identifiers and provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

Special categories of personal data (Article 9)

Special categories of personal data under the GDPR relates to:

- Racial or ethnic origin of the data subject
- Political opinions
- Religious or philosophical beliefs
- Trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Physical or mental health
- Sexual life
- Genetic or biometric data for the purpose of uniquely identifying an individual (e.g. Photos, fingerprints, facial recognition).

Personal data relating to criminal convictions and offences or related security measures based on criminal records can only be processed if there is a lawful basis for doing so (Article 6(1) of GDPR) and the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects (Article 10)

Personal data that has been pseudonymised – e.g. key coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Consent – is a freely given, specific and informed agreement by a Data Subject to the processing¹ of personal data about her/him. Consent under the GDPR must be freely given, specific, informed and an unambiguous indication of an individual's wishes. There must be some form of clear affirmative action – a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and there must be a simple way for people to withdraw consent.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 2018 and the General Data Protection Regulation 2016

4.0 GENERAL DATA PROTECTION REGULATION

4.1 Overview

The General Data Protection Regulation came into force on 25th May 2018 and describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images) and may include facts or opinions about a person. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) which became part of UK law from 25th May 2018.

¹ Processing – means collecting, amending, handling, storing or disclosing personal information.

5.0 RESPONSIBILITIES UNDER THE GENERAL DATA PROTECTION REGULATION

5.1 Data Controller

Concrete Rose will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data and determines what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

5.2 Data Protection Officer (DPO)

Concrete Rose has a Data Protection Officer (currently the Operations Lead) who will ensure that any concerns regarding the data held by Concrete Rose (including how it is stored and processed) are addressed. The DPO is also responsible for the day-to-day data protection matters including ensuring that all members of staff, volunteers, hosts and relevant individuals abide by this policy. The DPO is also responsible for ensuring that its notification with the Information Commissioner is kept accurate.

5.3 Wider responsibilities

Compliance with the legislation is the personal responsibility of all agents of Concrete Rose who process personal information. Individuals who provide personal data to Concrete Rose are responsible for ensuring that the information is accurate and up to date.

6.0 DATA PROTECTION PRINCIPLES

6.1 Overarching principles

Concrete Rose regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those we work with. The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles outlined below:

1. Process personal data fairly, lawfully and in a transparent manner

Concrete Rose will make all reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purposes of the processing, and any disclosures to third parties. We must ensure we have legitimate grounds for collecting data, use it transparently, and handle it only in ways individuals would reasonably expect.

2. Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.

Concrete Rose will ensure that the reason for which it collected the data originally is the only reason for which it processes that data, unless the individual is informed of any additional processing before it takes place.

3. Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

Concrete Rose will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data is given by individuals, it will be destroyed immediately.

4. Keep personal data accurate and, where necessary, up to date.

Concrete Rose will review and update all data on a regular basis and at least annually. Every reasonable step will be taken to ensure that personal data that is inaccurate is erased or rectified without delay.

5. Only keep personal data for as long as necessary.

Concrete Rose undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation. This will be governed strictly by the corporate retention schedules outlined in Section 11.0 of this policy.

6. Process personal data in accordance with the rights of the data subject under the legislation.

Individuals have rights to be told what information is held, prevent processing causing damage or distress, prevent direct marketing, and request rectification, blocking, erasure, or destruction of inaccurate data.

7. Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

Concrete Rose will ensure that all personal data is accessible only to those who have a valid reason for using it.

8. Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Concrete Rose will not transfer data to such territories without the explicit consent of the individual. This also applies to publishing information on the internet – because transfer of data can include placing data on a website that can be accessed from outside the EEA – so Concrete Rose will always seek the consent of individuals before placing any personal data (including photographs/videos) on its website.

If Concrete Rose collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

7.0 INFORMATION SECURITY

7.1 Data storage

Security is a critical part of keeping information confidential. Concrete Rose takes steps to ensure that all information is held securely both physically and electronically.

Concrete Rose will have in place appropriate security measures including:

- Keeping hard copies of all personal data in a lockable cabinet with key-controlled access.
- Password protecting personal data held electronically.
- Archiving personal data which is then kept securely.
- Placing any PC's or terminals that show personal data so that they are not visible except to authorised staff.
- Ensure that PC screens are not left unattended without a password protected screen-saver being used.

In addition, Concrete Rose will put in place appropriate measures for the deletion of personal data – manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PC's will be wiped

clean before disposal of and if that is not possible destroyed physically. A log will be kept of the records destroyed.

8.0 DATA COLLECTION

8.1 Lawfulness of processing (Article 6 (1)):

Concrete Rose does not rely solely or excessively on consent to process personal data. For processing to be lawful, Concrete Rose maps each processing activity to at least one of the following valid legal bases under Article 6 of the GDPR:

- **Consent:** The data subject has given clear, affirmative consent for a specific purpose (e.g., marketing or optional community engagement).
- **Contract:** Processing is necessary for the performance of a contract to which the data subject is party (e.g., staff employment contracts, host agreements, service delivery).
- **Legal Obligation:** Processing is necessary for compliance with a legal obligation to which Concrete Rose is subject (e.g., tax, payroll, safeguarding, health & safety reporting).
- **Vital Interests:** Processing is necessary to protect the life or critical health of the data subject or another individual (e.g., acute medical emergencies involving young people in accommodation).
- **Public Task:** Processing is necessary for the performance of a task carried out in the public interest.
- **Legitimate Interests:** Processing is necessary for the commercial or operational interests pursued by Concrete Rose, except where overridden by the rights and fundamental freedoms of the data subject (e.g., general business administration, securing funding, and monitoring initiative performance).

8.2 Consent as a basis for processing (Article 7)

Where consent is utilized, Concrete Rose ensures it is freely given, specific, informed, and unambiguous. Consent cannot be inferred from silence, pre-ticked boxes, or inactivity. It must be separate from other terms and conditions, and individuals must be provided with a simple, penalty-free mechanism to withdraw their consent at any time. If consent is withdrawn and no alternative lawful basis applies, processing will cease immediately.

9.0 DATA BREACH NOTIFICATION AND REPORTING

9.1 Definition of a Personal Data Breach

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 transmitted, stored, or otherwise processed.

9.2 Incident triage & reporting procedures

In the event of a suspected or confirmed personal data breach, the following strict regulatory timeline and workflow must be executed by the Data Protection Officer:

- **Internal Escalation:** Any staff member, volunteer, or host who discovers a data breach must report it to the Data Protection Officer (Operations Lead) immediately upon detection.
- **Notification to the Information Commissioner's Office (ICO):** The DPO must assess the risk to individuals. If the breach is likely to result in a risk to the rights and freedoms of individuals, Concrete Rose must report the breach to the ICO within 72 hours of becoming aware of it.
- **Notification to Data Subjects:** If the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, Concrete Rose must notify the affected data subjects without undue

delay, explaining the nature of the breach and recommended mitigation steps in clear, plain language.

- **Internal Breach Log:** Concrete Rose maintains an immutable, central Data Breach Register. Every incident—regardless of size, severity, or reportability—must be documented internally, noting the facts surrounding the breach, its effects, and the specific remedial actions implemented.

10.0 DATA SHARING

10.1 Types of data sharing

There are two types of data sharing: systematic and exceptional. 'Systematic' means a routine sharing of data or pooling of data. 'Exceptional' is one-off sharing (which might have to happen in an emergency). When deciding whether to share data, Concrete Rose will consider objectives, data minimization, strict "need-to-know" access principles, security of transmission, and potential risks to the individual.

10.2 Data Sharing Agreements

Data Sharing Agreements between Concrete Rose and external organisations must be formalised and make specific reference to the purpose of sharing, recipients, data quality, security protocols, retention limits, and mechanisms for handling data subjects' rights.

10.3 Exceptional data sharing

Concrete Rose complies with statutory guidelines on sharing information including compliance with the Prevent duty under the Counter-Terrorism and Security Act 2015. Information will be shared without consent where necessary to prevent death or serious harm, coordinate safeguarding responses, or protect vulnerable programme participants.

11.0 DATA STORAGE & RETENTION SCHEDULES

11.1 Retention policy & Principle

Personal data must not be kept by Concrete Rose for longer than is necessary to achieve the specific purposes for which it was originally collected. To formalize this, Concrete Rose operates under a strict, structured corporate retention schedule.

11.2 Corporate retention schedule

Personal data held by the organisation is categorised and subject to the following maximum retention periods:

Data Category / Record Type	Maximum Retention Period	Statutory / Regulatory Driver
Tax, Payroll & Financial Records	6 years following the end of the financial year	UK Taxes Management Act 1970 / HMRC Auditing Rules
Staff Employment Contracts & Personnel Files	6 years post-termination of employment	Limitation Act 1980 (Breach of Contract claims)
Unsuccessful Recruitment Records	6 months from date of appointment decision	Equality Act 2010 (Defending discrimination claims)

Young People Accommodation & Casework Records	7 years after the engagement or placement ends	Safeguarding compliance and Limitation Act 1980
Funding & Grant Records (Outcomes & Evaluations)	6 years following completion of the funded programme	Contractual terms of funding bodies and financial auditing
Volunteers & Hosts Operational Files	3 years post-termination of relationship	Operational management and liability defense
Health & Safety Accident Books / Incident Logs	3 years from date of last entry (or 40 years if hazardous exposure)	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR)

11.3 Secure destruction

Upon the expiration of the retention periods outlined above, data must be rendered non-recoverable. Hard copy records must be securely shredded or treated as confidential waste. Electronic records, server archives, and backups must be permanently deleted using secure deletion software. Redundant hardware must be physically destroyed or completely overwritten before disposal, and a centralized destruction log must be updated.

12.0 DISCLOSURE

12.1 Sharing with authorised agencies

Concrete Rose may share data with other agencies such as the local authority, funding bodies and other voluntary agencies. The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are statutory exemptions where the law allows Concrete Rose to disclose data without the data subject's consent, including carrying out a legal duty, protecting vital interests, or conducting legal proceedings.

13.0 SUBJECT ACCESS REQUESTS (SARs)

13.1 Access rights and compliance timelines

All Data Subjects have the right to access any personal data relating to them which are held by Concrete Rose. Any individual wishing to exercise the right should apply in writing to the Board of Directors.

- **Verification:** Concrete Rose must verify the identity of the requester before disclosing any records to prevent unauthorized access.
- **Statutory Deadline:** Under the strict terms of the UK GDPR, Concrete Rose must comply with and fully respond to a valid SAR **within one calendar month** of receipt. This response is provided free of charge, unless the request is manifestly unfounded or excessive.

13.2 Scope of a SAR

A Subject Access Request entitles an individual to receive a complete copy of their personal data, alongside formal notification of whether personal data is being processed, a description of the data categories, the specific reasons for processing, and details regarding any third-party recipients or data sources.

14.0 CHILD PROTECTION AND DATA ACCESS

14.1 Handling sensitive safeguarding data

Child protection and safeguarding information will be stored and handled with enhanced security measures in line with the DPA 2018 and UK GDPR principles. The legislation does not prevent staff from sharing information with relevant statutory agencies where that information may help to protect a child or vulnerable person.

Child protection records are normally exempt from standard disclosure provisions under individual rights if sharing the data would likely prejudice the prevention or detection of crime or compromise the child's vital safety interests. If any member of staff receives a request to see child protection records, they must refer it immediately to the Designated Safeguarding Lead, who will consult with Cambridgeshire County Council's Information Governance Team before a disclosure decision is made.

ADDENDUM 1: COVID-19 AND DATA PROTECTION

In order to best respond and help support the community response for COVID-19, it may be necessary for Concrete Rose to collect basic details from users and participants. Staff may be asked for sensitive personal data regarding underlying illnesses or shielding status to prevent the spread of the virus and protect those most vulnerable.

Any data collection implemented under this addendum will remain strictly limited to what is proportionate and necessary in accordance with active Government guidance to effectively keep people safe, maintain business continuity, and protect the wider community of Concrete Rose. Health data will be stored securely with a high duty of confidentiality, updated with the date of test results to ensure accuracy, and anonymized whenever communicating potential risks to colleagues.