



The Cambridge Acorn Project

DATA PROTECTION POLICY & PROCEDURE

Scope of Policy

This Policy covers all Subject Data held by The Cambridge Acorn Project either in paper or electronic format and the way it is handled. This policy covers our approach to case recording and to the processing of data under the terms of the Data Protection Act 1998 and the General Data Processing Regulation 2018.

Relevant Legislation:

The Data Protection Act 2018

UK GDPR

The Children Act 1989

The Children Act 2004

Safeguarding of Vulnerable Groups Act 2006

General Data Processing Regulation 2018

1. Introduction

This policy sets out in a clear and concise way to our staff, Trustees and volunteers exactly how we will handle data within our organisation and makes explicit our duties to our service users.

We are committed to:

- Holding information in a safe and secure manner and only using the information for the purpose for which it was given.**
- Keeping data up to date and accurate.**
- Recording fact not opinion.**
- Sharing information with other agencies only where we need to, for example for safeguarding reasons, or when we have the explicit consent of our service-users to do so.**
- Ensuring that all those we have data on understand the process for viewing what we have written about them if they wish to see it.**

- Removing out of date data from our records and disposing of it securely.
- Reviewing our policy on a regular basis to ensure that it still meets the needs of the organisation and its service users and is in conformity and up to date with legislation.
- Ensuring that we have informed consent from our service-users to process their data as part of their engagement with our service.
- Training all of our staff to ensure they have the knowledge of their, and our, obligations under the Data Protection Act 2018 and the UK GDPR.

2. Data Collection

Why we collect data

We primarily collect information:

- Regarding the work we do with service-users to ensure that our practice is safe, open, accountable and subject to the relevant monitoring.
- To meet safeguarding standards.
- As a means of reflectively thinking about the complex nature of our work in order to advocate for disadvantaged children and families and improve and enhance practice and service delivery.
- Quality Assurance Purposes – for example, collected SDQs or YP CORS.

We also collect information:

- Which we are required to report to funders under Grant Terms or Service Level Agreements (for example).
- To provide market segmentation of the above information.
- On our staff to enable us to manage our staff policies and payroll.
- On other contacts to help us run our business efficiently.

We may also collect information in the future:

- For research purposes. If this is the case we will ensure it meets the relevant ethical standards and will be fully anonymised and only used with explicit and informed consent.

How we collect data

We collect information from:

- Relevant work we do with service-users including, but not limited to, face-to-face contact, telephone calls, text messages, referral forms, emails and faxes. Not all

work is recorded and there must be clear expectations when and why work with children and families is (or is not) recorded.

- Application Forms
- Contacts we make at meetings, from emails or email networks
- Online research

3. The Data Controller

The designated Data Controller will deal with the implementation of the agreed policy and day to day matters. The Cambridge Acorn Project has a designated Data Controller, Matt Edge [07507740057], and is registered with the Office of the Information Commissioner.

4. Storing and Processing data

4.1 Our policy is to store all data in a secure manner and to dispose of data no longer required in a secure way. We will process data in a way which is consistent with the aims of our organisation and the purpose for which the data was given and with the informed consent of our service users.

4.2 Data in paper form will be kept in filing cabinets which will be kept locked overnight and when not in use. Data in paper format will be shredded before it is disposed of.

- Electronic data will be password protected and encrypted and be stored in a computer which will be locked away every night. All confidential and sensitive data pertaining to clients must be securely stored in our encrypted system, Tresorit which offers end-to-end encryption and is market-leading software in data protection (which we have assessed as superior to Ms OneDrive or Google Drive and other platforms). Note also the personal device at work section below.

4.3 We have a system in place for ensuring that any identifying data which leaves our premises, or is handed to us off-site (at a meeting for example), is checked in, and then locked away, every night.

4.4 We have the following procedures in place for case recording by practitioners on our system:

4.4.1 - All child protection concerns, as well as all concerns involving the safeguarding of a vulnerable adult (including self-harm), must be recorded within 24 hours.

4.4.2 - All other cases recording must be done as soon as is possible, in line with (for example) HCPC ethical standards of practice. We set a limit of (in total) **ten working days** on this. If recording is to be outside of these timescales, staff should inform the COO and Data Controller, Matt Edge.

4.5 Bring Your Own Device guidance

Typically this relates to smart phones, tablets and USB memory sticks.

4.5.1 Data stored by the Cambridge Acorn Project should never be transferred to a personal device unless the device is protected by a password (encryption is required if the data relates to information that would identify an individual) and permission for the transfer has been given by the Cambridge Acorn Project's Data Controller [Matt Edge]. Agreement must be reached as to how long the data may remain on the device. This will only be done in exceptional, mutually agreed, circumstances where complete security and encryption are guaranteed.

4.5.2 Client data must not normally be recorded on personal devices. With the use of encrypted 'cloud' services (Tresorit), this should not, besides, be necessary.

4.5.3 Great care must be taken when utilizing Tresorit that files are correctly downloaded and stored as per the online training video and the procedure which is also discussed as part of induction. Any practitioner unsure of this process should discuss with their supervisor as it is a clear risk of data loss if working on a shared computer and using Tresorit.

4.5.4. When transferring data from personal devices ensure you are using a secure channel. Public wi-fi networks may not be secure.

5. Retention of data

5.1 The Cambridge Acorn Project will keep some forms of information longer than others. We will need to keep central personnel records for 6 years after employment ceases. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

5.2.1 For general cases not covered under 5.2.2 or 5.2.3, we shall retain case records for 10 years.

5.2.2 For cases which have included a child protection referral/incident/suspicion/plan (of any kind) we shall retain the data for fifteen years. The primary reason being that we must remain accountable, as an organisation, for this work.

5.2.3 For cases which involve a young person in care, we shall retain the records for 25 years in line with standard practice. The primary reason for this is in case the young person concerned wants to do life-story work of some kind in the future.

6. Processing sensitive information

6.1 Sometimes it is necessary to process sensitive information about a person such as race, gender or family details (for example, on a referral form). This is done to ensure that the Cambridge Acorn Project can operate policies on matters such as sick pay or equal opportunities. We may also ask for information about particular health needs or disabilities. The Cambridge Acorn Project will only use such

information in the protection of the health and safety of the individual, but will need consent to process - for example, in the event of a medical emergency.

6.2 Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, employees and others affected will be asked to give express consent for the Cambridge Acorn Project to do this.

7. Disclosure

7.1 It is our policy not to disclose any information to third parties unless we have the subject's permission to do so OR the information is being passed solely for the third party to undertake work on our behalf and for no other purpose OR the information is already in the public domain OR we are legally obliged to do so, as is the case, for example, when there is a safeguarding concern to a child or an adult at risk of harm, as this will always override data protection principles.

7.2 Information will not normally be disclosed. Where information is being passed to a third party undertaking work on behalf of the organisation we will ensure that the third party has appropriate data protection policies and procedures in place.

8. Rights of the individual to access information (Subject Access Requests)

8.1 Employees and service-users of the Cambridge Acorn Project have the right to access any personal data that is being kept about them either on computer or in other types of files. Should any person wish to exercise this right they should contact the Data Protection Controller (Matt Edge).

8.2 In order to gain access, a request should be made in writing to the Data Controller (Matt Edge). The Cambridge Acorn Project reserves the right to make a charge of up to £10 on each occasion that access is requested.

8.3 The Cambridge Acorn Project aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days following receipt of a written request.

9. Inaccurate Data

Where an individual advises that any data we have recorded about them is inaccurate we will ensure the inaccuracy is corrected within 7 working days.

10. Complaints

Any complaints about the way we handle or use data will be dealt with under our Complaints Procedure.

11. Overseas Transfer

It is our policy not to transfer any data overseas.

12. Conclusion

12.1 Compliance with the Data Protection Act 2018 and UK GDPR is the responsibility of all staff, volunteers and Trustees of the Cambridge Acorn Project. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to our facilities or services being withdrawn, or even a criminal prosecution.

12.2 Any questions or concerns about the interpretation or operation of this Policy should be taken up with the Data Controller (Matt Edge).

Appendix 1

The following is a description of the information we have given the Office of the Information Commissioner:

Description of processing

The following is a broad description of the way this organisation/data controller processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have received, check any privacy notices the organisation has provided or contact the organisation to ask about your personal circumstances.

Reasons/purposes for processing information

We process personal information to enable us to provide health services to our patients, to maintain our accounts and records, promote our services and to support and manage our employees.

Type/classes of information processed

We process information relevant to the above reasons/purposes.

This information may include:

- personal details
- family details
- lifestyle and social circumstances
- goods and services
- financial details
- employment and education details

We also process sensitive classes of information that may include:

- physical or mental health details
- sexual life
- racial or ethnic origin
- trade union membership
- religious or other beliefs of a similar nature

- offences and alleged offences

Who the information is processed about

We process personal information about our:

- patients
- customers and clients
- staff
- suppliers
- business contacts
- professional advisers

Who the information may be shared with

We sometimes need to share the personal information we process with the individual concerned and also with other organisations.

Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA).

What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Where necessary or required we share information with:

- healthcare professionals
- social and welfare organisations
- central government
- business associates
- family, associates and representatives of the person whose personal data we are processing
- suppliers and service providers;
- financial organisations
- current, past and prospective employers;
- employment agencies and examining bodies

Appendix 2:

Casework Recording Guidelines

The running case record should include:

- A referral form **MUST** be sent before any casework can take place.
- A clear and consistent record of ongoing contact with the child, family and other professionals. It is not necessary to record general discussions, unless these have a notable impact on case development. There are, of course, no exceptions with child protection.
- Details of other professionals involved.
- Dates, times and, where appropriate, lengths of contacts.
- Child protection concerns clearly highlighted in a different colour, preferably red.
- Initials and time/date for when the record(s) were entered. If the case record is out of recording timescales (see above), then highlight the date and initials in yellow. Persistent and ongoing breaching of recording timescales, following a period of time and support given to address and correct this, may result in disciplinary action, where it is evidenced that practice has become negligent.
- Emails should not be cut and pasted.
- Clinical judgement should be used, in conjunction with supervision, about the level of detail required in recording individual cases. For example, a case which is in social care will require a greater level of detail for transparency and accountability reasons.
- It should always be remembered that this is the *child's record* (or, the adult's record), intended to provide a full account of the work the child does with the Cambridge Acorn Project, as well as providing clear accountability to them for our practice.

Example:

01/01/01, 9AM-10AM

Referral Meeting, School (Attending: Practitioner, Head Teacher, Social Worker, Senco, Parent)

Record of meeting...

Record of meeting

10/01/01, 9:15AM (10 mins)

Phone call from headteacher

AA disclosed physical abuse to his class teacher yesterday afternoon from a family member. Social care have been informed.

20/01/01, 15:16PM

Email from Mum

Saying that she would like to talk to me about the concerns raised in school last week. I have replied saying that I will call her tomorrow.

Appendix 3

Document retention periods relating to staff and accounts

Record	Statutory retention period	Statutory authority and/or Reason for retention
Personnel files including records and notes of disciplinary and grievance hearings	6 years from the end of employment	Potential litigation and references
Application forms/interview notes (unsuccessful applicants)	At least 6 months from the date of the interviews	Time limits on litigation
Facts relating to redundancies where less than 20	6 years from the date of the redundancy	Time limits on litigation
Accident books, accident records/reports	3 years after the date of the last entry (see below for accidents involving chemicals or asbestos)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (amended April 2012) (SI 1995/3163) as amended
Accounting records	3 years for private companies, 6 years for public limited companies	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631)
Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)

Record	Statutory retention period	Statutory authority and/or Reason for retention
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) (Amendment 2005) as amended
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the End of the tax year to which they relate	The Statutory Sick Pay (General) (Amendment) Regulations 2008
Wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970
National minimum wage records	3 years after the end of the pay reference period following the one that the records cover	National Minimum Wage (Amendment) Regulations 2011
Records relating to working time	2 years from date on which they were made	The Working Time Regulations 1998 (SI 1998/1833) Working Time Regulations (Amendment) Regulations 2009

COO – Matt Edge, matt@cambridgeacornproject.org.uk, 07507740047

**Safety and Compliance Officer, Mark Dalton,
mark@cambridgeacornproject.org.uk, 07503169144**

Trustees:

Pippa Ecclestone (Chair), pippa@cambridgeacornproject.org.uk

Chris Pugh (Treasurer)

Nichole Gibson

Fiona Nolan, fiona@cambridgeacornproject.org.uk

Latest revision: April 2023

To be revised: September 2024 (or earlier if the legal position changes or circumstances and practice learning require us to review earlier)

SIGNED BY THE PERSON LEGALLY RESPONSIBLE FOR THIS POLICY: Matt Edge, 24/04/2023