



## **Croydon Youth Information & Counselling Service Limited**

# **Data Protection Policy**

Croydon Drop In  
Tel: 020 8680 0404  
Company Limited by Guarantee Registration Number 3092355  
Registered Charity Number 1049307  
Registered Office, 132 Church Street, Croydon, CR0 1RF

---

*Through CDI's Policy Review System, all policies are reviewed annually from the date of approval*

# Data Protection Policy

## 1. Introduction

Croydon Drop In (CDI) is a registered Charity, supporting young people and families providing Information, Advocacy, Counselling, Outreach and Health Support in Communities & Schools.

CDI is the Data Controller for the purposes of the Data Protection Act 2018 and the General Data Protection Regulation 2016 (GDPR).

CDI is registered with the Information Commissioner's Office (ICO) as Croydon Youth Information & Counselling Service Ltd and the registration reference is ZA315283. The ICO is an independent body set up to uphold information rights.

CDI needs to gather and use certain information about individuals that engage with CDI services. This policy describes what, how and why information is collected and how it is used and stored in order to demonstrate compliance with data protection law. Personal data is defined as any information that can be used to identify an individual. CDI collects and uses certain types of personal information about the following categories of individuals (known as Data Subjects) that engage with CDI:

- Employees and prospective employees through recruitment
- Volunteers and prospective volunteers
- Trustees
- Children, young people and other individuals accessing CDI for support
- Parents/carers of service users
- Donors
- Local stakeholders, supporters and friends, and any other individuals who come into contact with the Charity.

## 2. Data Protection Principles

CDI is committed to processing data in accordance with its responsibilities under the GDPR. The UK GDPR sets out six key principles stating that personal data shall be:

- used fairly, lawfully and transparently
- used for specified, explicit and legitimate purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

## 3. CDI collect the following information

- Basic personal data includes, name, date of birth, email address, postal address and telephone numbers.
- Special categories of data is more sensitive personal information including ethnic background, religious beliefs, health, gender or sexual orientation.
- Presenting concerns of individuals accessing CDI services for support.
- Financial details (bank account number, UK tax payer information) of CDI employees and individuals making donations to the Charity.

---

*Through CDI's Policy Review System, all policies are reviewed annually from the date of approval*

- Technical data which may identify device IP address or web browser, via engagement with CDI's website and social media platforms.
- The use of CCTV outside CDI's offices for safety and security purposes.

#### 4. How CDI collect information

Most of the personal information CDI processes is provided to us directly by the individuals for the following reasons:

- They have contacted one of CDI's services and are accessing CDI for support.
- They have engaged with CDI's recruitment process, whether by sending their CV and/or completing a job application form.
- They have visited CDI's website, social media platforms or emailed CDI.
- They have attended an event hosted by CDI, such as CDI's AGM.
- They have made a donation to CDI.

For individuals accessing CDI services for support we may also receive personal information indirectly, from the following sources; Child & Adolescent Mental Health Services (CAMHS) / GPs and other health professionals / education providers / other professionals working alongside the individuals.

Practitioners who need to video record sessions for Training purposes whilst enrolled at University or approved Training Providers must follow this guidance.

- The recording must be completed using the practitioner's CDI work phone or laptop/Surface Pro (all devices must be password protected)
- Practitioners must gain consent from all clients who are recorded and they must sign the consent sheet (see appendix A, B and C)
- Practitioners must provide clients with a copy of the information sheet from their University or Training provider - see Appendix B and C
- The video must be stored securely on the practitioner's Microsoft Teams CDI account or University account which are always password protected
- The video must only be shown to Supervisors and/or in registered Tutor groups
- The video must not be uploaded eg. to personal accounts & social media platforms
- The video must be deleted at the end of the University/Training course
- The video may be uploaded for Training provider assignments if consent is given
- The video must not contain the name of our organisation (CDI/Croydon Drop In)
- The video must not contain any details that identifies the client, identifies their geographical location or compromises their anonymity

#### 5. Why CDI collect information

- To help provide the best service to all individuals that are involved with or access CDI services for support. As well as to signpost individuals to other services that can provide appropriate support.
- To collate and produce reports that CDI are required to write for service commissioners and funding providers such as CDI Quarterly Service Reports, CDI Annual Reports and funding applications. Personal data such as, gender identity, age, ethnicity, post code (first 3/4 letters/numbers only) and presenting concerns are always presented anonymously in reports. This information is included to ensure the support CDI provides is reaching the community in which CDI work.

- CDI receives funding from NHS England for some CDI service provisions. CDI are therefore required to provide monitoring information about individuals that access CDI services. This information is processed via NHS Digital; information does not include names but does include date of birth and postcode to ensure data is only accounted for once. Individuals accessing CDI services will always be asked for consent to share information with NHS Digital. It is an individual's right to decline to share their information with NHS Digital.
- Regular monitoring questionnaires and session notes are used to record how individuals accessing CDI services are feeling to ensure appropriate support is offered.
- Feedback/evaluation forms from individuals accessing CDI services for support are used to provide important information on service provision. CDI present these quotes anonymously and only when permission is given to do so.
- CDI use equal opportunity monitoring forms for recruitment and staff/service user surveys in order to gain information to ensure CDI are fulfilling equal opportunities.
- To analyse and improve services offered on CDI's website and social media platforms.
- To record and respond to any feedback or comments from any individuals involved with CDI.

## 6. Lawful purpose

Under the General Data Protection Regulation (GDPR), all data processed by CDI must be done on at least one or more of the following six lawful bases:

- **Consent:** the individual has given clear consent for CDI to process their personal data for a specific purpose. For example, allowing CDI to contact them via email or SMS. Individuals are able to remove consent at any time by contacting the CDI Director, via email [enquiries@croydondropin.org.uk](mailto:enquiries@croydondropin.org.uk) or writing to Croydon Drop In, 132 Church Street, Croydon, CR0 1RF.
- **Contract:** CDI may process personal data as part of an agreement CDI has with the individual. For example, a contract of employment.
- **Legal obligation:** CDI may collect or share an individual's personal data where CDI is required to do so by law. For example, relating to safeguarding.
- **Vital interests:** CDI may use an individual's personal data if there is an immediate risk to their health or safety.
- **Public task:** Some of CDI's activities are undertaken in the public interest. For example in the area of public health.
- **Legitimate interests:** CDI's legitimate interest is to support children, young people and families regarding mental health and wellbeing. This means that the reason we are processing information is because there is a legitimate interest for CDI to do so to ensure we provide the most appropriate support.

## 7. Sharing information

CDI does not share the information provided to any individuals or organisations without express permission from the individual(s) concerned. In line with CDI's Confidentiality Policy and CDI's Safeguarding Policy there are however, exceptional circumstances whereby CDI may need to act without permission including; if we feel someone is at risk to themselves or to others, in an emergency or when ordered to by a court of law. CDI will act in consultation with, and in the best interests of our clients, and reserves the right to refuse to share information following consultation and may only release information on receipt of a subpoena. CDI will, wherever possible, keep individuals informed with any actions taken.

CDI will never sell or share personal information to any organisations for marketing purposes.

## 8. Storage of information

CDI take all steps reasonably necessary to make sure that personal data, whether in paper or electronic form, is treated securely. Information at CDI is stored on password protected secure databases, secure password protected server and any paper records are held in secure locked filing cabinets.

Information will only be accessed by authorised personnel, including those who are responsible for supporting individuals accessing CDI services, relevant CDI staff members and those responsible for maintenance and security of CDI's digital systems. Please also refer to the CDI Acceptable Information Technology Use Policy for additional information and guidance.

In the event of potential data security incidents such as emergency situations including, electronic system failure, flood or fire please refer to the CDI Business Continuity Plan.

## 9. Retention and disposal of information

CDI only keeps an individual's information as long as reasonable and necessary for the relevant activity. CDI are legally required to hold some personal data to fulfil statutory obligations. After the relevant time all data is sensitively and securely deleted and/or destroyed in the most appropriate way. At the end of this policy document Appendix A – CDI Data Retention outlines certain data retention periods to be complied with.

## 10. Individual's (Data Subject's) Rights

The Data Protection Act 2018 and UK GDPR provides the following rights for individuals:

- **The right to be informed about how their data is being used:** CDI has the responsibility to be clear about the collection, processing, use, sharing and retention of personal data. This is provided in CDI's Privacy Statement, which CDI regularly review and update where necessary.
- **The right to access their personal information:** Individuals have the right to request access to a copy of the personal information that CDI holds about them in many circumstances. This is referred to as a 'Subject Access Request'. All requests must be made in writing to the CDI Director at: Croydon Drop In, 132 Church Street, Croydon, CR0 1RF.

CDI will request proof of identity and sufficient information about the individual's interactions with CDI in order to locate their personal data. Please note, some of these rights only apply in certain circumstances. Where one of the rights does not apply CDI will communicate the reason to the individual. If CDI agree that they are obliged to provide personal data to the individual (or someone else on their behalf where consent is provided), CDI will provide it and aim to do so 30 days from when identity has been confirmed. No administration fee will be charged for considering and/or complying with such request unless the request is deemed to be excessive in nature.

- **The right to correct their personal information:** Individuals can ask CDI to change or complete any inaccurate or out of date personal information held about them by CDI.
- **The right to restriction, objection and erasure:** Individuals can ask CDI to restrict the personal information used about them and/or object to the processing of their personal data in some circumstances. Individuals can ask CDI to delete their personal information where it is no longer necessary for CDI to use it or they have withdrawn consent. This is also known as the 'right to be forgotten'. These rights are not absolute and only apply in certain circumstances.
- **The right to data portability:** Individuals can ask CDI to provide some of the personal information held about them in a structured, commonly used and electronic format so it can be easily transferred.
- **The right to no automated decision-making:** Automated decision-making takes place when an electronic system uses personal information to make a decision without human involvement. CDI do not currently carry out any automated decision-making.

In accordance with GOV.UK instruction there are some situations when organisations are allowed to withhold information, e.g. if the information is about, the prevention, detection or investigation of a crime. An organisation does not have to say why they are withholding information.

## 11. Breaches

In the event of any and all breaches of GDPR, this should be reported to the CDI Director as soon as it is discovered.

The following will then be assessed:

- the extent of the breach
- the risks to the data subjects as the consequence of the breach
- any security measures in place that will protect the information
- any measures that can be taken immediately to mitigate the risk to individuals.

Unless there is unlikely to be any risk to individuals from the breach, it must be reported to the Information Commissioner's Office (ICO) within 72 hours, where feasible, of the breach coming to the attention of the Charity.

We are registered with the Information Commissioner as Croydon Youth Information & Counselling Service Ltd and our registration reference is ZA315283.

The Information Commissioner's Office is at: <https://ico.org.uk> and their helpline no. is 0303 123 1113

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, CDI must also inform those individuals without undue delay.

CDI must keep a record of any personal data breaches, regardless of whether CDI are required to notify. Please refer to the CDI Data Incident Policy for further information.

## 12. Responsibilities and Training

Everyone who works/volunteers for/with CDI should adhere to this Data Protection Policy and has the responsibility for ensuring data is collected, stored and handled appropriately.

The CDI Board of Trustees, CDI Director and CDI Senior Management Team are ultimately responsible for ensuring that CDI meets its legal obligations. This includes but is not limited to:

- Ensuring the review and update of the CDI Data Protection Policy and CDI Privacy Statement.
- Ensuring the review and update of all associated policies and risk assessments concerning data management and protection, including the CDI Business Continuity Plan, CDI Data Incident Policy and the CDI Acceptable Information Technology Use Policy.

The CDI Director is the first point of contact regarding all Subject Access Requests.

The CDI Director and CDI Deputy Director are responsible for ensuring that:

- CDI's IT provider, SME IT Solutions, is compliant and ensures all systems, services and equipment meet acceptable security standards and are reviewed on a regular basis.
- All other third party providers, for example, HR/Payroll Company, Appointment Management System, CCTV security provider adhere to all data protection legislation.

The CDI Deputy Director, in collaboration with line managers, is responsible for ensuring relevant induction processes and training requirements are adhered to.

All CDI employees, volunteers and trustees are required to complete annual data protection training. Evidence of training course completion e.g. certificates are required to be submitted to the CDI staff members' line manager. All training certificates are to be recorded on the HR database.

## 13. Additional information

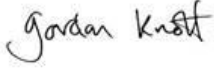
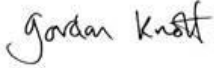
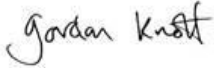
This policy should be read in conjunction with the following:

- CDI Privacy Statement
- CDI Confidentiality Policy
- CDI Safeguarding Policy
- CDI Acceptable Information Technology Use Policy
- CDI Data Incident Policy
- CDI Business Continuity Plan
- CDI Risk Register
- CDI Data Retention table (Appendix A in this Policy)

If you need to find out more about this policy please contact the CDI Director by emailing [gordon@croydondropin.org.uk](mailto:gordon@croydondropin.org.uk)

The Information Commissioner's Office (ICO) regulates data protection and privacy matters in the UK. Additional information is available on their website <https://ico.org.uk/>

## POLICY REVIEW

Policy Prepared by	Date Prepared	Policy Approved by	Date Approved	Approved Signature	Review Date
Anna Austin (Data Lead)	Re-written June 2022	Gordon Knott – CDI Director	June 2022		June 2023
Policy Reviewed by	Date Reviewed / Amended	Policy Approved by	Date Approved	Approved Signature	Review Date
Gordon Knott	21 <sup>st</sup> June 2023	Gordon Knott – CDI Director	June 2023		June 2024
Policy Reviewed by	Date Reviewed / Amended	Policy Approved by	Date Approved	Approved Signature	Review Date
Gordon Knott	07.03.24	Gordon Knott – CDI CEO	March 2024		March 2025

---

*Through CDI's Policy Review System, all policies are reviewed annually from the date of approval*



## Appendix A – CDI Data Retention

This appendix is to be read and adhered to in relation to the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Data / Document	Action
CDI Human Resource Records	<p>CDI must keep human resource records for at least 6 years.</p> <ul style="list-style-type: none"> <li>• Personnel files and training records (including formal disciplinary records) retention period: 6 years after employment ceases.</li> <li>• Working time records including overtime, annual holiday, jury service, time off for dependents retention period: 2 years from date on which they were made.</li> <li>• Senior Management Team records may be needed permanently for historical purposes.</li> <li>• Recruitment application forms and interview notes (for unsuccessful candidates) retention period: 6 months to a year.</li> </ul>
CDI Financial and Accounting Records	<p>CDI must keep records about the Charity and financial and accounting records for 6 years from the end of the last company financial year. If records are lost, stolen or destroyed CDI must:</p> <ul style="list-style-type: none"> <li>- do the best to recreate them</li> <li>- tell the Corporation Tax office straight away</li> <li>- include this information in the Company Tax Return.</li> </ul> <ul style="list-style-type: none"> <li>• Payroll wage/salary records retention period: 6 years from the end of the tax year to which they relate.</li> <li>• Statutory Maternity Pay records retention period: 3 years after the end of the tax year in which the maternity period ends.</li> </ul>
CDI Operational Documents	<ul style="list-style-type: none"> <li>• CDI Board of Trustees Meetings minutes retention period: permanently, during the existence of the Charity.</li> <li>• Health and Safety logs, such as accident records, retention period: 3 years from date of the last entry (or, if the accident involves a child/young person, then until that person reaches the age of 21).</li> <li>• First Aid training retention period: 6 years after employment.</li> <li>• Fire Warden training retention period: 6 years after employment.</li> <li>• Subject Access Requests retention period: 1 year following completion of the request</li> <li>• Whistleblowing documents retention period: 6 months following the outcome (if a substantiated investigation).</li> </ul>
CDI Service User Records:	<p>Service users/parent/carer information is to be kept for the duration of contact with CDI services and archived thereafter for a period of 6 years, prior to shredding/electronic disposal. This is in line with guidance from British Association for Counselling and Psychotherapy to reflect professional liability and legal requirements.</p> <p>It is necessary to keep some records for longer in compliance with legal requirements, such as safeguarding, child protection and children looked after.</p>

### Sources and additional information:

[www.gov.uk/data-protection-your-business](http://www.gov.uk/data-protection-your-business)

[www.ico.org.uk/for-organisations/](http://www.ico.org.uk/for-organisations/)

[www.cipd.co.uk/knowledge/fundamentals/people/hr/keeping-records-factsheet](http://www.cipd.co.uk/knowledge/fundamentals/people/hr/keeping-records-factsheet)

---

*Through CDI's Policy Review System, all policies are reviewed annually from the date of approval*