# Data Protection and Confidentiality Policy

## Practical rules for handling information safely across CIRC activities

| Document control | Details |
|---|---|
| Organisation | Community Integration & Recovery Centre (CIRC) C.I.C. |
| Document owner | Data Protection Lead |
| Effective date | 17 September 2026 |
| Next review | 17 September 2027 |
| Status | Approved website version |

**Purpose and status.** This document sets the standard expected by Community Integration & Recovery Centre (CIRC) C.I.C.. It should be read with applicable law, contractual requirements, local safeguarding procedures and related operational procedures. It does not replace professional judgement or legal advice in a specific case.

## Policy statement

CIRC requires authorised, minimum-necessary access; accurate and respectful records; secure communication; confidentiality in every setting; and immediate reporting of mistakes or suspected compromise. These rules apply to directors, staff, contractors, volunteers, students and partners handling CIRC information.

## Day to day handling rules

| Activity | Required practice |
|---|---|
| Collecting | Use approved forms and systems; explain the purpose; collect only what is necessary; record the source and consent where relied upon. |
| Accessing | Access only records needed for current duties. Never browse from curiosity, use data personally or share accounts or passwords. |
| Recording | Write promptly, objectively and respectfully. Separate fact, report and opinion. Correct mistakes transparently without hiding the audit trail. |
| Email and messaging | Use approved accounts; verify recipients; use BCC for unrelated bulk recipients; minimise attachments; use secure transfer for sensitive material. |
| Events and sign-in | Avoid displaying unnecessary contact details; protect registration lists; collect accessibility information |

| Activity | Required practice |
|---|---|
| | separately where appropriate. |
| Photography and recording | Use approved devices and documented authority; provide notice; record separate consent where relied upon; store and delete securely. |
| Paper and remote work | Keep records attended or locked; protect screens and conversations; use approved storage; do not use personal cloud or messaging without authority. |
| Sharing | Confirm identity, authority, purpose, lawful basis and minimum dataset; record significant disclosures; use suitable agreements. |
| Disposal | Apply the retention schedule and legal holds; securely shred paper and erase or destroy media and devices. |

## Sensitive participant information

Information about health, immigration or sponsorship experiences, ethnicity, religion, disability, sexuality, domestic circumstances, employment disputes or vulnerability can create particular harm if disclosed. It must be collected only for a defined purpose, restricted to people who need it and never included in public reports, case studies or partner updates unless lawfully anonymised or expressly authorised.

## Confidentiality and safeguarding

Confidentiality is not absolute. Relevant information may be shared to deliver an agreed service, comply with law, protect vital interests, safeguard a person, prevent or detect crime or respond to an authorised regulator or court. Staff and volunteers must not delay an urgent safeguarding disclosure because consent is unavailable. They must share only what is necessary and record what was shared, why, with whom and under whose authority.

## Rights requests complaints and corrections

Any request for access, correction, deletion, restriction, portability, objection, withdrawal of consent or review of an automated decision must be sent to the Data Protection Lead on the day received. Relevant records must be preserved and deletion must not be promised. Privacy complaints must be acknowledged, investigated, documented and answered with information about escalation to the ICO.

## Security incidents

Report immediately any lost device or paper, misdirected message, exposed mailing list, unauthorised access, inappropriate conversation, phishing, malware, altered or unavailable record, accidental deletion, excessive disclosure or insecure disposal. Do not wait for proof or conceal the incident.

1. Contain safely, recall messages where possible, secure affected accounts or materials and preserve evidence.
2. Notify the manager and Data Protection Lead immediately using the incident route.

3. Record what happened, the people and information affected, timing, recipients, controls and actions.
4. Do not contact affected people, the ICO, media or other third parties unless authorised.
5. Cooperate with risk assessment, notification, recovery and learning.

## Access retention and enforcement

Managers authorise access based on duties, review permissions regularly and remove them promptly when roles change or end. Record owners apply the retention schedule and pause deletion during a complaint, safeguarding concern, investigation, litigation or other legal hold. Training is mandatory for relevant roles. Noncompliance may lead to retraining, access restriction, disciplinary or contract action, external referral or legal action.

## Authoritative sources

This document was prepared with reference to the following official sources. The online version of each source should be checked at review or following a material legal or regulatory change.

**Information Commissioner's Office. Guide to data protection.** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/
**Information Commissioner's Office. Contracts and liabilities between controllers and processors.** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/contracts-and-liabilities-between-controllers-and-processors-uk-gdpr/
**UK legislation. Data Protection Act 2018.** https://www.legislation.gov.uk/ukpga/2018/12/contents
**UK legislation. Data Use and Access Act 2025.** https://www.legislation.gov.uk/ukpga/2025/18/contents