GDPR Compliance Policy

Accountability framework for lawful and transparent personal data processing

Document control	Details
Organisation	Community Integration & Recovery Centre (CIRC) C.I.C.
Document owner	Directors and 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.

Scope and objectives

This policy applies to CIRC's directors, employees, contractors, sessional workers, volunteers, students and partners when they process personal data for CIRC. It covers information about participants, beneficiaries, referrers, event attendees, donors, supporters, workers, applicants, professionals, suppliers and website users in paper, electronic, audio, visual or verbal form. Its purpose is to embed the UK GDPR principles and demonstrate accountability across CIRC's programmes and corporate activities.

Governance and responsibilities

Role	Core responsibilities
Directors or Board	Approve this policy, set risk appetite, provide resources, challenge assurance and oversee serious incidents.
Founder or lead Director	Ensure data protection is integrated with strategy, partnerships, public communications and accountability.
Data Protection Lead	Maintain records of processing, notices, lawful-basis records, DPIAs, rights handling, incident records, training and advice.
Programme and project leads	Define necessary information, control access, maintain quality and retention, and apply approved safeguards.

Role	Core responsibilities
All workers and volunteers	Use information only for authorised purposes, protect confidentiality, follow procedures and report incidents immediately.

Data protection principles

1. Process personal data lawfully, fairly and transparently.
2. Collect it for specified, explicit and legitimate purposes and avoid incompatible use.
3. Use only information that is adequate, relevant and limited to what is necessary.
4. Keep information accurate and correct material errors without undue delay.
5. Retain identifiable information only for as long as necessary.
6. Protect confidentiality, integrity and availability through appropriate security.
7. Maintain evidence that demonstrates compliance.

Lawful processing

Before processing begins, the responsible lead must document the purpose, Article 6 lawful basis and any Article 9 or criminal-offence-data condition. Consent is used only where people have genuine choice and withdrawal can be honoured. Legitimate interests require a necessity and balancing assessment. Sensitive information concerning health, immigration experiences, race, religion, disability or vulnerability must not be collected without a defined need, lawful condition and appropriate safeguards.

Processing decision	Required evidence
Ordinary personal data	Purpose and Article 6 lawful basis.
Special category data	Article 6 basis plus Article 9 condition and any DPA 2018 Schedule 1 requirement.
Criminal-offence data	Article 6 basis plus Article 10 authority and applicable DPA 2018 condition.
New high-risk project	Approved DPIA before launch.
Research or evaluation	Purpose, lawful basis, transparency, minimisation and research safeguards.
Processor appointment	Due diligence and Article 28-compliant written terms.
International transfer	Transfer mechanism, transfer assessment and supplementary measures.

Transparency and individual rights

Clear privacy information must be provided at or before collection and, when information comes from another source, within the applicable timeframe unless an exemption applies. Any rights request must reach the Data Protection Lead on the day received. Identity checks must be proportionate, searches

reasonable, exemptions documented and responses normally issued within one month. Privacy complaints will be investigated fairly, documented and answered with information about escalation to the ICO.

Data protection by design and DPIAs

New programmes, referral pathways, research, monitoring, online services, databases, fundraising tools, artificial intelligence and data-sharing arrangements must consider privacy from the outset. Default settings should minimise collection, access, publication and retention. A DPIA is required before processing likely to create high risk, including large-scale sensitive data, systematic monitoring, innovative technology or linked datasets with significant effects.

Records, retention and security

The Data Protection Lead maintains appropriate records of processing. Record owners apply the retention schedule, legal holds and secure disposal. Security controls must reflect the risks to migrants, workers, people experiencing hardship and others who could be harmed by disclosure. Suspected loss, misdirection, unauthorised access, disclosure, alteration, cyberattack or unavailable records must be reported immediately. The ICO will be notified without undue delay and, where feasible, within 72 hours when the legal risk threshold is met; affected people will be informed where the risk is high unless a lawful exception applies.

Sharing, suppliers and international transfers

Sharing must be necessary, proportionate, secure and documented. CIRC will verify the recipient, purpose, lawful basis, minimum dataset and any safeguarding need. Processors require due diligence, written Article 28 terms and ongoing assurance. Joint-controller arrangements must transparently allocate responsibilities. Restricted international transfers require approval and a lawful safeguard.

Training, monitoring and review

Relevant workers and volunteers complete induction and refresher training. Compliance is monitored through audits, incident trends, rights performance, DPIAs, access reviews, supplier assurance and Board reporting. Deliberate or negligent noncompliance may lead to access restriction, retraining, disciplinary or contract action, regulatory reporting or legal action. This policy is reviewed annually and after a significant legal, service, technology or risk change or serious incident.

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