WE CREATE UNITY CIC

Privacy & Data Protection Policy

Stronger Together. Better Communities.

Organisation	We Create Unity CIC
Company number	16541073
Registered office	34 The Market Square, London, England, N9 0TZ
Organisation type	Community Interest Company
Version	1.0
Reviewed	October 2026
Review cycle	At least annually and when material legal or operational changes occur

1. Controller and scope

We Create Unity CIC, company number 16541073, registered office 34 The Market Square, London, England, N9 0TZ, acts as controller where it decides why and how personal data is used. The Board must assign a privacy lead and publish a monitored contact route. This internal policy complements, but does not replace, a concise public-facing privacy notice.

2. Data handling principles

Collect only information needed for a defined purpose, explain lawful bases, keep records accurate, restrict access, secure systems and delete or anonymise information when retention ends. Maintain a record of processing activities proportionate to WCU's processing.

3. Lawful bases and sensitive data

Identify an Article 6 lawful basis for each purpose; for health, safeguarding or other special-category information identify an Article 9 condition and, where relevant, a Data Protection Act 2018 Schedule 1 condition and appropriate policy document. Do not assume consent is always the appropriate safeguarding basis.

4. Forms, media and children

Website registration and contact forms must explain purposes, recipients and retention, and avoid unnecessary sensitive details. Obtain appropriate permissions for identifiable photographs, video, audio and testimonials; provide a withdrawal/contact process where applicable. Use age-appropriate notices and additional protection for children.

5. Security and processors

Use access controls, multi-factor authentication, strong credentials, restricted sharing, secure backups and documented access removal. Before using Hostinger, Stripe, Microsoft, Google or other processors, check contracts, security, international transfer safeguards and data roles. Do not transmit safeguarding case details in routine notification emails.

6. Rights requests and breaches

Log and verify rights requests; ordinarily respond within one month, subject to lawful extensions and exemptions. Record personal data breaches, contain and assess them promptly; notify the ICO within 72 hours of awareness where a reportable risk threshold is met and notify affected individuals where high risk requires it.

7. Retention and disclosure

Approve a category-specific retention schedule for enquiries, project attendance, financial records, staff files, media and safeguarding information. Apply statutory, contractual and safeguarding requirements rather than a blanket deletion period. Document disclosures to agencies and partners.

8. Marketing, cookies and accountability

Obtain consent for non-essential cookies and apply PECR requirements to electronic marketing. Maintain a cookie notice and consent mechanism where required. Assess whether ICO data protection fee registration applies; document DPIAs for processing likely to present high risk.

9. Scope and responsibility

This policy applies to directors, employees, contractors, sessional workers, volunteers and representatives acting for WCU, including online activity and delivery with partners. The Board is accountable for implementation; a named policy lead will coordinate operational arrangements.

10. Implementation and assurance

All relevant personnel will receive induction appropriate to their role, confirm that they have read this policy, and report concerns or breaches promptly. The Board will review implementation, record significant decisions and ensure corrective actions are followed up.

11. Review and implementation

This policy will be considered at the next WCU governance meeting and reviewed at least annually, or sooner following material operational or legal changes. Directors should record interim adoption and

any subsequent amendments in meeting minutes. The review date above must be confirmed against the organisation's actual review records.