Privacy Notice

Bugle Library of Things CIC | Organisation-wide data protection framework

Document reference	D01
Controller	Bugle Library of Things CIC (Company No. 12846276)
Owner	Harry Deacon — Data Protection Lead
Status	Final proposed text; Board adoption / outstanding factual checks as indicated
Effective date	03/11/2026
Scheduled review	Annually from approval; earlier if processing or law changes
Approval reference	R12-03-11-26

1. Who we are

Bugle Library of Things CIC (trading as BLoT) is a Community Interest Company registered in England and Wales, company number 12846276. Registered office: 48a Fore Street, Bugle, St Austell, Cornwall PL26 8PE. BLoT is normally the controller of information collected for its own services. Contact: hello@blotcic.org or 0800 009 6409. Data Protection Lead: Harry Deacon (an internal lead, not a formally designated statutory Data Protection Officer). ICO registration: [ICO REGISTRATION NUMBER — TO BE CONFIRMED].

2. Who and what this notice covers

This notice applies to visitors to our website, Community Hub and Mobile Hub; people seeking support; volunteers, applicants, employees and directors; donors, customers and lottery entrants; partner contacts; event participants; and people identified in referrals, safeguarding concerns, complaints, photographs or case studies. Role-specific notices or notices supplied when collecting information may provide further detail, particularly for staff, recruitment or safeguarding.

3. Information we may collect

- Identity and contact details; communication preferences; correspondence; support requests and proportionate case notes, including relevant staff observations and referrals.
- Information about attendance, activities, volunteering, employment, applications, governance and partner relationships.
- Donations, orders, lottery entries, transaction identifiers, financial records and payment status. Payments are handled using Stripe; BLoT does not need to receive or store complete card details.
- Optional demographic and evaluation answers; photographs, recordings, quotes and case studies where relevant.
- Where justified, information concerning health, disability, ethnicity or other special-category information; safeguarding disclosures, reports and possibly allegations of criminal offences.
- Website/device and technical information including logs, cookie choices and analytics only in accordance with the actual website configuration and applicable consent requirements.

4. Why we use information and lawful bases

Provide practical support and keep necessary case notes	Legitimate interests (Article 6(1)(f)): accessible, continuous and accountable community support; proportionate assessment of individual rights.

Support voluntary referrals	Legitimate interests where justified; permission to contact a partner is sought where practicable. Alternative bases may apply to particular arrangements.
Protect children and individuals at risk	Recognised legitimate interests (Article 6(1)(ea)) where statutory criteria are met; another lawful basis only where justified. Additional sensitive-data conditions below.
Optional identifiable monitoring	Consent (Article 6(1)(a)), with separate explicit consent for special-category data.
Donations, purchases and lottery administration	Contract (Article 6(1)(b)) where necessary to fulfil a transaction; legal obligation (6(1)(c)) for statutory records; legitimate interests for proportionate fraud-prevention and service administration.
Financial records and PAYE	Legal obligation, contract or legitimate interests depending on the activity and obligations.
Recruitment, employment and volunteers	Contract, steps requested before contract, legal obligation and/or legitimate interests depending on the particular activity.
Opt-in newsletters and fundraising marketing	Consent (6(1)(a)), with applicable electronic-marketing rules and unsubscribe controls.
Complaints, rights requests and incidents	Legal obligation where applicable; legitimate interests for fair handling, recordkeeping and service improvement.

5. Sensitive personal information, safeguarding and allegations

BLoT avoids routinely recording health, disability, ethnicity and other special-category details in ordinary support work. Where recording is needed for ordinary support and BLoT relies on explicit consent, we explain the specific purpose and obtain and record that consent. Information voluntarily disclosed is not automatically consent to retain it. People may withdraw consent, after which we review processing and deletion unless another independently valid condition applies. Optional identifiable sensitive demographic questions have a separate explicit opt-in; refusing does not affect support. Where a child or qualifying adult at risk needs protection, BLoT may process or share necessary information without consent if the legal conditions for safeguarding are met. Safeguarding records may contain factual accounts of alleged crimes. Allegations are recorded as allegations, not findings, with access strictly limited. BLoT assesses the legal basis for such information under Articles 6, 9 and/or 10 and the Data Protection Act 2018 as appropriate.

6. Monitoring, evaluation and case studies

Demographic monitoring is voluntary and distinct from support delivery. We use anonymous or aggregated statistics where practical and suppress small groups if identification is possible. Funders ordinarily receive aggregated results. Identifiable testimonials, photographs, case studies or sensitive personal stories are only shared for the agreed purpose with appropriate recorded permission and any additional lawful conditions.

7. Who we share information with

We may share limited information with partner organisations at the individual's request or where a lawful safeguarding or other justification applies; safeguarding authorities, emergency services, statutory services or police where necessary; professional advisers and accountants; service delivery and IT providers; and others needed for authorised transactions. We limit disclosures, verify recipients and keep a record where appropriate. David Jeffery & Co processes PAYE/payroll on our behalf and acts as an independent controller for its other accountancy services.

8. Our service providers and overseas processing

We use Microsoft 365 (including Microsoft Forms) for organisational records and forms, Microsoft Dynamics for CRM/donor management, Mailchimp for opted-in communications, SurveyMonkey for surveys, Stripe for payments and professional accountancy services. Free Google Forms are not used to collect new identifiable sensitive data under our adopted policy; any remaining use is assessed separately. Some providers may handle information outside the UK. Where a restricted international transfer occurs, BLoT must ensure an applicable adequacy mechanism or appropriate transfer safeguards. Supplier privacy notices provide more information about their own activities; they do not replace BLoT's responsibilities. Website-specific hosting and plugin disclosures will be confirmed against the live website before publication.

9. Security, forms and storage

Authorised staff access records on a need-to-know basis, with separate safeguarding records, role-based permissions and multifactor authentication. Paper notes are temporary and moved into suitable secure records. Sensitive emails are sent only to authorised organisational recipients; staff avoid unnecessary forwarding and use appropriately secure sharing methods. Form submissions may be emailed to authorised staff and manually incorporated into restricted records. Unnecessary duplicates are deleted as soon as practicable and within 90 days of verified transfer unless another justified requirement applies.

10. Retention

We retain records only for as long as justified for their purposes, subject to statutory requirements and case-specific holds. Different periods apply to financial, employment, support, lottery and safeguarding information. Safeguarding records have particular safeguards and retention criteria. Where records are no longer required, we securely delete, destroy or anonymise them. Contact us for further information about a particular category of record.

11. Communications and photography

Marketing is optional and requires the appropriate opt-in. Every electronic marketing message includes an appropriate unsubscribe route. Identifiable photographs and stories used externally require documented written or electronic permission and additional safeguards for children and sensitive circumstances.

12. Your rights

Subject to the conditions and exemptions in law, you may request access, correction, erasure, restriction, data portability or object to certain processing. Where we rely on consent you may withdraw it. We usually respond to data-subject requests within one calendar month, subject to lawful extensions and identity checks. Send requests to hello@blotcic.org. Rights are not absolute; for example, information may need to be retained for safeguarding or legal reasons.

13. Data protection complaints and contact

Contact Harry Deacon at hello@blotcic.org or 0800 009 6409 with privacy concerns. BLoT will acknowledge data protection complaints within 30 days and investigate and respond without undue delay in accordance with applicable legislation. You may also complain to the Information Commissioner's Office at ico.org.uk or 0303 123 1113. This notice is reviewed at least annually and whenever significant processing changes.

14. Cookies and website-specific information

A separate Cookie Policy explains cookies, analytics and how visitors may control consent. Non-essential technologies must be used consistently with applicable consent requirements. The actual website plugins, cookie inventory, hosting, logs, embeds and retention settings will be checked with the website developer before this notice and the Cookie Policy are published.

15. Organisational privacy arrangements (approved policy)

For identifiable sensitive information in ordinary support work, BLoT generally avoids recording the detail unless specific, valid explicit consent is obtained, or another documented Article 9 condition applies. Consent to receive support is not automatically explicit consent to retain sensitive records.

Sensitive optional demographic questions are subject to separate recorded explicit opt-in; refusal or withdrawal does not affect support. Funders receive aggregated or effectively anonymised data by default. Identifiable stories and images require written or electronic permission.

BLoT uses organisational Microsoft Forms for identifiable sensitive surveys, not consumer Google Forms. When necessary information has been verified in its official restricted record, redundant form copies and notification emails are deleted promptly, no later than 90 days unless a documented exception applies.

Professional accountants David Jeffery & Co act as processor for PAYE/payroll under BLoT instructions and as independent controller for other accountancy services. Relevant responsibilities and agreements apply to each activity.