Privacy Data Protection and Media Policy

Creative Makers CIC

Policy leads: Rebecca Knee, Director, and Tom Knee, Data Protection Lead
Version: 2.0
Issue and signature date: 25 September 2026
Next review: 25 September 2027, or sooner if practice or requirements change

Supersedes the policy reviewed and signed on 1 January 2026. This revision updates digital record handling and links to the Information Security, Acceptable Use and Records Management Policy.

1 Policy statement and scope

Creative Makers CIC protects the privacy, dignity and personal information of children, young people, families, staff and partners. This policy applies to personal information used in providing creative alternative provision and related organisational activities.

We will handle information in accordance with the UK GDPR and Data Protection Act 2018, as amended. Staff must use information lawfully, fairly and transparently, for specified purposes, keeping it relevant, accurate, secure and no longer than necessary.

2 Responsibility and accountability

Rebecca Knee has overall responsibility for this policy. Tom Knee is the Data Protection Lead and coordinates access, records, enquiries and incident management. Staff must follow this policy, complete annual data protection training through their individual Prospero accounts and report concerns promptly.

Creative Makers CIC is the organisation responsible for its own controller activities; naming policy leads does not make those individuals the controller. For council-commissioned processing, the Data Protection Lead will confirm and document whether Creative Makers acts as controller, joint controller or processor for each activity, and the relevant agreement with the council. This relationship remains to be confirmed for the due diligence questionnaire.

The Data Protection Lead will maintain a record of processing purposes, information categories, recipients, legal grounds, storage, access and retention decisions. New systems or significant changes must be checked for privacy risks, including whether a data protection impact assessment is needed.

3 Purpose and types of information

We use information to safeguard children, provide appropriate support, communicate with families, respond to medical needs, record attendance and progress, and meet relevant legal, commissioning and insurance requirements. We collect only what is necessary.

Records may include names, dates of birth, addresses, parent/carer and emergency contacts, medical needs and allergies, SEND information and EHCPs, attendance, safeguarding concerns, session notes, progress reports, and incident or accident records. Photographs and videos may also be personal information. Health and disability information require additional protection; criminal offence information has separate legal safeguards.

4 Lawful use and transparency

Before processing information, the Data Protection Lead must record an appropriate lawful basis for each purpose. Health and other special category information also require a relevant additional condition. Where

applicable, the corresponding Data Protection Act condition and an appropriate policy document must be in place. These grounds must be checked against our actual functions and commissioning arrangements rather than assumed.

Children, young people and families must receive clear, accessible privacy information about who uses their data, why, who receives it, retention, rights and contact routes. Consent is used where appropriate, particularly for optional promotional media, but is not treated as the basis for every activity. Refusing optional publicity must not affect access to provision.

5 Storage and confidentiality

Our records are held digitally in a paid Google Workspace subscription, using Google Forms, Drive, Docs and Sheets. Staff have individual creative-makers.co.uk accounts. Folder permissions limit access to the children they work with and the information necessary for their role.

Paper is not routinely retained. Where information is captured on paper, it is promptly scanned or photographed using an approved device, saved to the correct restricted folder and checked for completeness and readability. The original is then shredded unless a documented requirement or preservation instruction requires it to be retained. Any such temporary original must be secured and accessible only to authorised staff.

Staff must protect devices, avoid unnecessary downloads and discuss children and families privately. The companion Information Security, Acceptable Use and Records Management Policy sets out the detailed rules. Technical settings and hosting arrangements must be verified by the Data Protection Lead; a paid subscription alone is not evidence that every security control is configured.

6 Information sharing

Staff may share information only for an authorised purpose, with an appropriate recipient and through approved secure channels. Before sharing, check the recipient, the minimum information needed, the legal grounds and any relevant restrictions. Record significant disclosures and the reason for them.

Necessary safeguarding information may be shared without consent where there is an appropriate legal basis. Staff must follow safeguarding procedures and must not promise absolute confidentiality. Data protection concerns must not delay urgent safeguarding action.

The Data Protection Lead will confirm council and supplier arrangements, including instructions where Creative Makers acts as a processor, applicable contracts, hosting locations and safeguards for any international transfers.

7 Retention and disposal

Records are retained according to the Retention Schedule in the companion policy and any applicable legal, safeguarding or commissioning requirements. Each record category must have a justified retention period or clear disposal criterion and a review point.

Some category-specific periods still require confirmation with the council, safeguarding lead and insurer. Pending decisions must be actively resolved; they do not authorise indefinite retention. Staff must not delete records subject to a safeguarding preservation instruction, complaint, claim, investigation or information request. The Data Protection Lead will record disposal decisions and arrange secure deletion or destruction.

8 Photography video and media

Written permission appropriate to the child or young person and the proposed use must be obtained before optional photographs or videos are taken. Separate choices must distinguish private family sharing, learning records and publicity. Staff must explain the audience and purpose, respect the young person's wishes and check safeguarding restrictions.

Promotional publication requires specific consent. Children's full names must not appear alongside published images. Staff must not use personal social media or unapproved personal cloud accounts to store or share images. Images must be stored in restricted organisational folders and reviewed when their purpose ends or consent changes.

Consent for future use may be withdrawn. We will stop further use and remove material from channels we control where appropriate, explaining any limits on recalling material already distributed. Permission records must be retained for as long as needed to evidence authorised use. Media is not kept indefinitely merely because consent was once obtained.

9 Website and online privacy

The website must provide an accurate privacy notice reflecting actual collection and use of data. Any cookies or similar technologies must be reviewed and managed under the applicable rules, including obtaining consent where required. New forms, online services and website changes must be checked for privacy and security before use.

10 Individual rights and requests

Children and young people have rights over their own personal information. Parents and carers do not automatically have unrestricted access to a child's records. The Data Protection Lead must check identity, authority, the child's understanding and wishes, their best interests, third-party information and applicable restrictions.

Requests may concern access, correction, deletion, restriction, objection, portability or withdrawal of consent, depending on the circumstances and legal basis. Staff must send requests promptly to Rebecca Knee or Tom Knee and must not insist on a particular form or wording. Subject access requests are normally answered without undue delay and within one month, with any lawful adjustment or extension assessed and communicated.

Requests and data protection complaints can be directed to Tom Knee at Tom@creative-makers.co.uk or 07708 334788. Concerns can also be raised with the Information Commissioner's Office. Erasure is not automatic where there is a lawful reason to retain information.

11 Data breaches

Staff must immediately report lost devices, misdirected messages, unintended sharing, suspected unauthorised access or other possible breaches to Rebecca Knee or Tom Knee. Preserve relevant evidence and follow containment instructions.

The Data Protection Lead will record the incident, assess the risk and coordinate action. Where Creative Makers is a controller, a reportable breach must be notified to the ICO without undue delay and, where feasible, within 72 hours of awareness. Affected people must be informed without undue delay where the breach is likely to pose a high risk. Where Creative Makers is a processor, the relevant controller must be informed without undue delay. Decisions, reasons and corrective actions must be recorded even where external notification is unnecessary.

12 Review and implementation

This policy is reviewed annually and following relevant changes, significant incidents or changes in services. The Data Protection Lead will confirm outstanding legal grounds, council processing roles, supplier arrangements and retention decisions, and brief staff on the revised requirements.

Read alongside the Staff Code of Conduct and Safer Working Practice Policy, safeguarding arrangements, and the Information Security, Acceptable Use and Records Management Policy.

Signature

Signed: Rebecca Knee
Director, Creative Makers CIC
Date: 25 September 2026
Typed signature

Reference guidance

ICO guidance on special category information
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/special-category-data/

ICO guidance on subject access
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/subject-access-requests/a-guide-to-subject-access/

ICO guidance on personal data breaches
https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/