Information Security Acceptable Use and Records Management Policy

Creative Makers CIC

Policy leads: Rebecca Knee, Director, and Tom Knee, Data Protection Lead
Version: 1.0
Issue and signature date: 25 September 2026
Next review: 25 September 2027, or sooner if practice or requirements change

Includes Appendix A, Retention Schedule, and Appendix B, Implementation Checks. New requirements in this policy must be put into practice; unverified settings are identified in Appendix B.

1 Purpose and scope

This policy sets out how Creative Makers CIC protects information, uses digital systems and manages records throughout their life. It applies to staff, practitioners, volunteers and others authorised to access organisational information, at all venues and when working remotely.

It supports the Privacy, Data Protection and Media Policy and Staff Code of Conduct. It covers council-referred children's information, family details, EHCPs, health information, attendance, safeguarding, progress and operational records. Staff must follow the stricter applicable safeguarding or contractual restriction where one applies and ask the Data Protection Lead to resolve conflicts.

2 Responsibilities and current arrangements

Rebecca Knee, Director, has overall responsibility. Tom Knee, Data Protection Lead, coordinates implementation, permissions, supplier checks, retention decisions and incidents, with technical assistance where needed. Staff are responsible for protecting their accounts and devices and reporting concerns immediately.

Confirmed current arrangements are a paid Google Workspace subscription; Google Forms, Drive, Docs and Sheets; individual organisational accounts; restricted folders based on the children staff work with; digital records with paper digitised and shredded; and annual Prospero data protection training. All relevant staff have enhanced DBS clearance.

Hosting countries, two-step verification settings, device controls, recovery arrangements and any certification remain unverified. This policy sets requirements; it does not certify that all technical controls are already enabled.

3 Accounts and access permissions

Use only your individually assigned organisational account for work information. Do not share accounts, passwords or verification codes. The Data Protection Lead must authorise access according to role and need, restrict administrative privileges and maintain a record of permissions.

A staff member may access only information needed for their assigned work. Safeguarding and particularly sensitive records require additional restrictions. Folder ownership must remain under organisational control. Review access when responsibilities or placements change and at least each term. Remove access promptly when a person leaves or no longer needs it; preserve and transfer organisational records before closing an account.

4 Passwords and two step verification

Use a unique password for the organisational account, avoiding names, dates of birth or other predictable personal details. The new organisational standard is at least 14 characters, using a long passphrase such as three unrelated words or an approved password manager's generated password. Do not reuse work passwords elsewhere. This minimum is an organisational choice to implement, not a statement about a verified current setting.

Do not require routine password changes solely because time has passed. Change a password immediately if compromise is suspected, it has been disclosed, or the Data Protection Lead instructs you after an incident. Do not impose predictable substitutions or reliance on complexity alone.

Two-step verification must be enabled for staff accounts, with priority for administrator accounts. The Data Protection Lead must verify and document enforcement, approved recovery methods and safe storage of recovery codes. Staff must never approve an unexpected sign-in prompt. If a control cannot yet be implemented, the Director must record the gap, interim restrictions, owner and completion date.

5 Devices and working locations

Access work information only on devices approved by the Data Protection Lead. Devices must have a passcode or password, automatic screen locking, supported software and timely security updates. Encryption and protection against malicious software must be enabled where appropriate and checked. Lock screens whenever unattended and protect devices from theft.

Personal devices require prior approval and a check that work information can be kept separate from personal accounts and removed when access ends. Family members must not be able to access work information. Avoid local downloads, offline copies and removable drives unless specifically authorised. Do not automatically back up work files or photographs to personal cloud services.

Work where conversations and screens cannot be overheard or viewed by unauthorised people. Use trusted connections or an approved secure method; do not use shared public computers for children's information. Report a missing or compromised device immediately.

6 Acceptable use of systems and communication

Use approved organisational systems and professional communication channels. Do not contact pupils through personal social media or share personal contact details. Do not forward work information to personal email accounts.

Check recipients and access permissions before sending or sharing information. Prefer restricted links to authorised recipients, give the least necessary access and avoid publicly accessible links. Check Google Forms response destinations and sharing settings before collecting information. Limit sensitive content in email subjects and collect only information needed for the stated purpose.

Do not upload children's information to unapproved apps, public AI tools, personal messaging services or personal storage. New tools, extensions and integrations need approval before they access organisational data. Staff must not bypass security controls, install unapproved software, use systems unlawfully, or access records out of curiosity.

Be alert to suspicious attachments, links, payment requests and unexpected sharing invitations. Verify unusual requests through a known contact route and report concerns rather than attempting to investigate alone.

7 Recording storing and updating information

Create clear, accurate records promptly, identifying the author and date and distinguishing observation, reported information and professional opinion. Use agreed folder names and record identifiers. Keep one authoritative record and avoid unnecessary duplicate files.

Store records in the correct restricted Google Workspace location. Check accuracy with appropriate sources, record corrections transparently and retain significant earlier versions where needed for accountability. Keep safeguarding records separate or more tightly restricted in accordance with safeguarding procedures.

Scan or photograph temporary paper using an approved device. Check every page is readable and complete and saved to the correct location before shredding the original. Remove unnecessary device copies and temporary images after confirming the organisational copy is secure. Retain an original only where a legal, safeguarding or contractual requirement requires it, and secure it with restricted access.

Maintain a record inventory covering each category, its owner, purpose, location, access restrictions, relevant legal grounds, retention trigger and disposal decision. Record significant transfers to the council or another provider and obtain confirmation where appropriate.

8 Retention deletion and equipment disposal

Use Appendix A to manage review and disposal. The Data Protection Lead must confirm outstanding category-specific periods and document their authority. An annual review is a check point, not a substitute for a justified retention period. Apply holds for safeguarding, claims, investigations, complaints or information requests; record the reason and review date for each hold.

When disposal is authorised, delete records from relevant active locations and manage copies, trash, retention settings and backups according to the verified system arrangements. Do not promise immediate irreversible deletion from every provider copy. Record any residual retention and access restrictions. Retain a proportionate disposal log identifying the category, decision date, authority, method and person responsible, without reproducing unnecessary sensitive content.

Paper originals are shredded after verified digitisation. Before electrical equipment leaves organisational control, arrange verified secure data erasure or specialist destruction of data-bearing storage if erasure cannot be assured. Keep equipment secure pending disposal and retain appropriate disposal records or destruction certificates.

9 Suppliers recovery and continuity

Before introducing a supplier or materially changing a service, the Data Protection Lead must check contractual protections, access, storage and processing locations, international transfer arrangements and deletion terms. Confirm the countries relevant to the council's questionnaire rather than assuming a UK location or using a broad regional label.

Document how records can be recovered after accidental deletion, account compromise or service disruption, including the limits of Google Workspace features and any approved backup arrangement. Test the agreed recovery procedure periodically and after significant changes. Synchronisation and trash folders must not be assumed to provide a complete backup. Any additional service needs a privacy and security check before use.

10 Incidents and information requests

Report lost devices, wrong recipients, public links, unusual sign-ins, malware or suspected unauthorised access immediately to Tom Knee or Rebecca Knee. Do not conceal errors or erase evidence. Follow authorised containment instructions. Contact details: Tom@creative-makers.co.uk; 07708 334788.

The Data Protection Lead will log and assess incidents, coordinate recovery, inform the council where required and apply the notification procedure in the Privacy, Data Protection and Media Policy. Refer access, correction or deletion requests promptly to the leads; do not delete relevant records while a request is being assessed.

11 Training monitoring and review

Staff must complete data protection training annually through their individual Prospero accounts and receive an induction into these rules before access is granted. The Data Protection Lead will track completion and brief staff when procedures change.

The Director will review this policy annually and after significant incidents or operational changes. Permission checks, implementation actions and disposal decisions must be recorded. Failure to follow the rules is addressed through appropriate management and safeguarding procedures.

Appendix A Retention schedule

This schedule covers the information discussed for Creative Makers' provision. It is not authority to delete safeguarding or evidential records. Final retention periods for the categories marked below require recorded confirmation against commissioning terms, safeguarding requirements and insurer advice. The Data Protection Lead owns that work with the Director and safeguarding lead.

At adoption, identify records without an approved period, record a justified interim review date and resolve the decision promptly. Pending confirmation does not justify indefinite retention. Review active records for accuracy and necessity; review closed records at the relevant trigger and at least annually while retained. Record the final period and authority in the controlled schedule before automated deletion is enabled.

Record category	Review trigger	Retention and disposal decision
Referrals, EHCPs, health and family information	Placement ends, referral is declined or information is superseded.	Final period to confirm with council and safeguarding lead. Review historical need; do not discard records needed to explain decisions or concerns.
Attendance, session notes and progress reports	Placement ends or reporting obligation is completed.	Final period to confirm against commissioning, safeguarding and claims requirements. Record the agreed trigger and number of years or other defined endpoint.
Safeguarding concerns and associated evidence	Case closure, transfer or other approved safeguarding trigger.	Period and trigger to be confirmed by safeguarding lead using applicable guidance and council requirements. No routine deletion before that decision; check preservation instructions.
Accident, incident and complaint records	Incident or complaint closes; any claim is resolved.	Confirm period with insurer, safeguarding lead and applicable requirements, including the age of the child and unresolved claims. Apply any hold.
Temporary paper, scan images and duplicate downloads	Complete readable copy is verified in the restricted organisational record.	Shred paper and remove unnecessary temporary copies promptly after verification, unless an original or copy must be preserved.
Optional photographs and videos	Agreed purpose ends, placement changes or consent is withdrawn.	Review at each trigger. Stop unauthorised future use; delete copies no longer needed from controlled locations. Retain relevant evidence only for a separately justified purpose.
Media permissions and sharing decisions	Related use or disclosure ends.	Keep while needed to evidence authorised use; final subsequent period to be approved and recorded. Link to any relevant

Record category	Review trigger	Retention and disposal decision
		complaint or claim hold.
Staff training and access authorisations	Training is superseded, role changes or employment ends.	Remove access promptly when no longer needed. Confirm retention of evidence with employment, safeguarding and commissioning requirements.
Recruitment and DBS administration records	Recruitment decision or employment ends.	Use the safer recruitment policy and applicable DBS guidance. Confirm category-specific periods; do not keep certificate copies indefinitely or assume enhanced clearance justifies extra retention.
Breaches, rights requests and disposal logs	Incident or request closes or disposal is completed.	Approve a proportionate evidence period, taking account of complaints, accountability and any investigation. Record the period and review trigger.
Finance and governance records containing personal data	Accounting year closes or governance record is superseded.	Confirm applicable company, tax and contractual retention rules through financial controls and governance procedures. These records need their own justified periods.

Appendix B Implementation checks

Tom Knee will coordinate the following checks with Rebecca Knee and record completion, outstanding actions and target dates. These checks distinguish the policy requirements from settings not yet verified.

- Confirm the council processing role and relevant agreements for each activity, including lawful grounds for sensitive information.
- Confirm relevant Google Workspace hosting and processing countries, transfer arrangements, supplier terms and responses for questionnaire questions 2(e) and 3(b).
- Check and configure the password minimum and two-step verification, administrator access and account recovery. Record interim restrictions for unresolved gaps.
- Check device approval, encryption, screen locks, security updates and restrictions on local copies and personal cloud backup.
- Verify folder permissions, external sharing, Google Forms access and staff joining, changing role and leaving procedures.
- Confirm recovery and backup arrangements and test restoration; document deletion and trash retention behaviour.
- Approve category-specific retention periods and triggers in Appendix A with the council, safeguarding lead and insurer where relevant.
- Confirm any claimed security certification before including it in questionnaire question 3(c). No certification is asserted by this policy.
- Brief staff on the new requirements, record their acknowledgement and track annual Prospero training.

Signature

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

Reference guidance

NCSC guidance on password administration
https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

ICO guidance on storage limitation
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/storage-limitation/

ICO guidance on disposal and deletion
https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/toolkits/records-management/disposal-and-deletion/