

Records Retention & Destruction Policy

Keep With Purpose. Delete With Control. Preserve the Evidence.

Company: Right First Time UK Ltd | No. 17493370 | Accepted 3 October 2026 | Updated 13 October 2026

1. Purpose and scope

Right First Time UK Ltd (RFTUK) retains records where needed for lawful operations, accountability, financial administration, safeguarding, evidence, research and organisational continuity. It reviews, securely destroys or anonymises records once there is no justified reason to keep them.

This policy applies to paper, email, databases, applications, websites, messages, audio/video, financial records, cloud storage, server logs, backups and records held for RFTUK by authorised suppliers. It applies to Directors, Campaign Leaders, Volunteers, staff and contractors.

2. Retention principles and responsibility

Personal data must not be kept in identifiable form longer than necessary. There is no single UK GDPR retention period for all personal information. Each record type has an identified purpose, relevant legal basis, owner, retention trigger, default period and review or disposal action.

Directors oversee compliance; authorised record owners apply the schedule and ensure access controls. These default periods are not permission to keep unnecessary personal data. Statutory obligations, legal holds, safeguarding needs and properly documented risk assessments can change them.

3. When the clock starts

The retention period normally runs from the relevant trigger, not necessarily the date a record was first collected: for example, the end of the relevant financial year, meeting date, end of a contract, final complaint closure, the end of a role, last meaningful contact or the date a policy was superseded.

Where a retention period is expressed as a review date, the record owner must decide whether continued retention is justified, document the decision and set another review date.

4. Preservation and legal holds

Relevant records must be preserved during existing or reasonably anticipated litigation, investigations, tax enquiries, serious complaints, safeguarding reviews, subject access requests and regulatory processes. Records subject to a hold must not be concealed, altered or destroyed.

A legal hold must identify the records and responsible person, restrict changes appropriately, and remain in effect until formally released. Holds must be proportionate rather than indefinitely freezing unrelated records.

5. Company identity and statutory governance

The certificate of incorporation, registered Articles of Association, constitutional amendments and key company-identity records are kept for the life of the company and normally preserved in its historical archive. The registered Articles are the controlling constitutional document; this policy does not amend them.

Directors' meeting minutes and Members' resolutions/general-meeting records must normally be retained for at least 10 years under the Companies Act 2006. Statutory registers are maintained in accordance with their specific legal requirements. Public Membership and statutory company membership records are separate.

6. Financial, tax, donations and restricted funding

RFTUK normally keeps core financial and tax records, including ledgers, bank records, invoices, receipts, expense claims, membership-payment references, donations and tax returns, for six years from the end of the relevant financial year, or longer where a specific HMRC, grant, audit or investigation requirement applies.

The Companies Act minimum for private-company accounting records is generally three years from the date made; RFTUK applies the longer internal six-year financial standard. Restricted-fund and grant evidence remains available for the applicable funder audit, restriction or clawback period.

7. Contracts, suppliers and procurement

Material executed contracts and supplier records normally remain for six years after expiry, termination or the final relevant transaction, subject to legal holds or longer terms. Deeds, property rights, licences, intellectual-property assignments and continuing liabilities may need longer case-specific retention.

Supporting records may include quotations, approvals, conflict declarations, due-diligence results, security assessments, payment evidence, performance reviews and exit agreements. Low-risk records should not be stored longer simply because they are easy to keep.

8. Public Membership, subscribers and donations

Public Membership account information is kept while the membership operates. The minimum contract and payment records may then be kept for up to six years where justified; marketing history is reviewed separately and not automatically retained for that whole period.

Subscriber details are retained while subscribed. An opt-out or unsubscribe request removes the individual from active marketing, while a minimal suppression record may be retained to prevent re-subscription without permission. Donation financial records follow the financial schedule; unnecessary donor profiles do not.

9. Volunteers, staff and applicants

Volunteer, Campaign Leader and Campaigner records remain during the role, with ordinary role and access records normally reviewed three years after departure. Information relevant to financial authority, safeguarding, complaints or litigation may need up to six years or longer if justified.

Unsuccessful applications normally are deleted within six months after the final decision, or limited details can be kept for up to 12 months with an appropriate basis for future opportunities. Employment/worker, payroll, pension, health and safety and recruitment records are retained under the applicable specialist rules; six years after leaving may be an appropriate general default for core employment records where justified.

10. Complaints, privacy rights and whistleblowing

Ordinary complaint records are normally retained for three years after final closure. Serious legal, safeguarding, discrimination or financial cases may require up to six years or an individually justified longer period. Anonymous themes may be kept for learning.

Data-protection rights requests and complaints are normally kept for three years after closure unless under ICO review or proceedings. Identity evidence collected just for verification should be removed when no longer required.

Whistleblowing and serious speaking-up records require restricted access and a proportionate case-by-case review, ordinarily by six years after closure. The identity of a reporter should not circulate unnecessarily.

11. Safeguarding and DBS records

Safeguarding material is subject to documented case-specific retention and periodic review, taking account of the person's age, seriousness, ongoing risk, referrals and possible future evidence needs. No short universal period is imposed. Access must be tightly restricted.

DBS certificate data is processed in line with current DBS rules. Full certificates should not ordinarily be copied or retained when a proportionate record of the check outcome will suffice.

12. Research, media and published material

Source research and evidence are retained only as needed to substantiate public findings, check accuracy, respond to corrections and preserve legitimate campaign history. Unneeded identifiable information should be redacted or anonymised.

Final significant publications and the version history of material corrections can be retained as an organisational archive. Raw recordings and photographs require privacy, safeguarding, consent, copyright and need-based reviews rather than automatic permanent retention.

13. Websites, analytics, email and messaging

Routine identifiable website, firewall, server and security logs are normally reviewed for deletion or anonymisation within 12 months; an incident or legal hold can justify longer. Analytics settings must follow the applicable Website Analytics and Privacy notices.

Important email and messaging decisions should be stored in the proper organisational case or governance record. Duplicate attachments, low-value correspondence and unnecessary personal-device copies should be removed. Disappearing messages must not be used to defeat record-preservation duties.

14. Meetings, registers, policies and training

Approved minutes form the primary meeting record; draft notes and recordings may normally be removed when no longer needed. Material risk, conflict and gifts/hospitality register entries normally remain while active and for at least six years after closure where justified.

Approved superseded policies are normally preserved for at least six years, with important foundational versions kept longer. Ordinary training completion records are normally reviewed three years after role departure or the training being superseded, unless a role requires longer.

15. Cyber incidents, breaches and backups

Material cybersecurity and personal-data-breach records are documented sufficiently to show response, notification decisions, remediation and accountability. They are normally reviewed after six years; low-level alerts may have much shorter periods.

Backups are for recovery and use a documented rotation cycle, not indefinite archiving. Erased personal data must not be routinely restored into active systems without a legitimate reason. If required, legal holds can preserve relevant backups.

16. Secure disposal and anonymisation

Confidential paper must be shredded or destroyed securely; digital data must be removed with methods proportionate to sensitivity, such as secure deletion, encryption-key destruction or physical media disposal. The recycle bin alone is not enough for sensitive material.

A record can be anonymised where legitimate aggregate or historical value remains but identity is no longer necessary. Pseudonymised information is still personal data where re-identification is reasonably possible. Material destruction decisions may be logged.

17. Erasure and disclosure requests

Individuals may ask for erasure, but the right is not absolute where a legal duty, legal claim or another statutory exception justifies retention. Requests are assessed, explained and recorded. Relevant information must not be destroyed to frustrate a pending subject access request, complaint or investigation.

18. Annual review and responsible implementation

Key information stores are reviewed at least once a year, and higher-risk repositories more often. Reviews cover dormant accounts, duplicate files, archived databases, log settings, expired backups, obsolete identification copies, unresolved holds and access held by former team members.

The record owner applies this schedule; Directors supervise unresolved material risks. No person may destroy records to conceal wrongdoing or defeat a disclosure obligation.

19. Parent Contribution Service (PCS)

PCS is an RFTUK Ltd service, not a separate legal entity. RFTUK does not hold or transfer voluntary parent-to-parent contribution money; the PCS service-access charge is separate from those parent payments.

A dedicated PCS retention schedule and privacy notice must address member/parent/child account data, agreements and versions, messages, payment records provided by users, evidence uploads, safeguarding or safety-pause records, complaints and audit logs. High-risk material must be protected, and deletion must be purpose-based and subject to legal holds.

This organisation-wide policy does not create a blanket indefinite-retention period for PCS messages or family information. Any operational storage setting must be checked for consistency with the dedicated PCS privacy disclosures and applicable law.

20. Related policies, review and contact

Read with the RFTUK Privacy Notice, Data Protection & GDPR Policy, Information Security & Cybersecurity Policy, Financial Controls & Expenses Policy, Safeguarding Policy, Complaints Policy, Whistleblowing Policy and applicable PCS privacy documents.

This policy is reviewed at least annually and sooner following material legal, technical or safeguarding changes. Retention or evidence-preservation concerns may be raised through the Contact Us page. Data-protection complaints may also be directed to complaints@rightfirsttimeuk.com.

Appendix A. Default retention schedule

Periods are organisational defaults and require review where law, safeguarding, contract, an active complaint or a legal hold changes the need.

Record category	Default period or review	Main reason
Constitution and formation	Life of organisation / historical archive	Company identity and Articles
Directors' approved minutes	At least 10 years after meeting	Companies Act 2006
Members' resolutions and general meetings	At least 10 years	Companies Act 2006
Statutory company registers	As required by current law	Register and inspection duties
Tax, accounts, bank, invoices, receipts	Normally 6 years after financial year-end; longer if required	HMRC, financial accountability
Restricted funds and grants	At least 6 years, or longer funder term	Audit, funding conditions
Supplier and contract files	Normally 6 years after expiry/termination	Contract and evidence
Deeds and continuing rights	Case-specific, potentially longer	Long-term rights / liabilities
Public Membership payment records	During membership; then up to 6 years if justified	Consumer, accounts, disputes
Subscribers and suppression records	While subscribed; limited suppression after opt-out	Communications preferences
Volunteer / Campaigner files	During role; normal review after 3 years	Role administration
Higher-risk Volunteer records	Up to 6 years or longer if justified	Safeguarding / legal risk
Unsuccessful applications	Normally 6 months; up to 12 months with basis	Recruitment fairness
Core employee/worker records	Record-specific; often up to 6 years after leaving	Employment and tax obligations
Ordinary complaints	Normally 3 years after final closure	Complaints accountability
Serious/legal complaints	Up to 6 years or longer on review	Legal / safeguarding risks
Data-rights requests and complaints	Normally 3 years after closure	Regulatory accountability
Speaking-up / whistleblowing	Review ordinarily by 6 years after closure	Restricted investigation records
Safeguarding	Individual documented period and review	No universal period
DBS certificate information	Minimum lawful period	DBS requirements
Research and evidence	While needed; then review / anonymise	Accuracy, publication support
Major final publications	Long-term / historical archive	Public accountability
Routine identifiable security logs	Review within 12 months, often sooner	Security and minimisation
Material cyber / data breaches	Review after 6 years	Accountability and legal risk
Approved superseded policies	Normally at least 6 years	Historical standards
Training completion	Normally 3 years after leaving / supersession	Role evidence
Backups	Documented rolling backup cycle	Disaster recovery
PCS messages and uploads	Dedicated PCS schedule; specific justified periods	Privacy, safety, dispute evidence

Official references and contact

ICO - Storage limitation | GOV.UK - Company and accounting records | Companies Act 2006 s.248 - Board meeting minutes | Companies Act 2006 s.355 - resolutions and minutes | Limitation Act 1980 s.5 - simple contracts

Right First Time UK Ltd - Company No. 17493370. Registered office: 82A James Carter Road, Mildenhall, IP28 7DE, England. A non-profit company limited by guarantee, with no share capital.

Contact: <https://rightfirsttimeuk.com/contact-us.php> | Data-protection complaints: complaints@rightfirsttimeuk.com

PCS is an RFTUK service. The registered Articles of Association remain the controlling constitutional document.