Data Retention Policy and Schedule – October 2026

1. Purpose and Scope

1.1 This Policy sets out how long In-Form Solutions Ltd, a company registered in England and Wales under number 03961045, whose registered office is at 88 Hill Village Road, Four Oaks, Sutton Coldfield, West Midlands B75 5BE ("the Company"), keeps its records, and how they are reviewed and securely disposed of.

1.2 Personal data must not be kept for longer than is needed for the purpose for which it was collected. Keeping records for the right length of time also means the Company can meet its legal, tax, contractual and audit duties, and defend itself if a claim is made.

1.3 This Policy applies to all records held by or for the Company, in any format, and to everyone who works for or on behalf of the Company ("associated persons"). It forms the Company's records retention schedule referred to in the Information Governance Policy Suite (Version 08) and the Data Protection Policy Statement.

2. Where Records Are Kept

2.1 Company records are kept only in the following places:

- the Company's Microsoft 365 systems, including SharePoint, OneDrive and Outlook, accessed through Company accounts;
- Company-managed laptops and devices, for working copies only;
- the Company's finance and payroll systems; and
- locked storage at the Company's premises, for paper records.

2.2 Personal data must not be stored on personal devices or personal accounts. Associate consultants must keep all Company and client records in the Company's systems. During an assignment they may keep working copies on an approved, encrypted device, but must save them to SharePoint at least daily, keep no personal or patient data locally without approval, and delete local copies when the assignment ends.

3. Client Records and Data

3.1 Where the Company acts for a client, the client's contract and instructions decide how long client data is kept. If they are stricter than this Schedule, the client's rules apply.

3.2 At the end of each engagement, the engagement lead makes sure that any personal data the Company holds on the client's behalf (as its processor) is returned or securely deleted, as the contract requires. Patient-identifiable data, health information and HR information about client staff are never kept beyond the end of the engagement.

3.3 The Company's own client files, including contracts, proposals, correspondence, working papers, final reports and deliverables, are kept for 15 years after the engagement ends. This is the longest period in which a claim for negligence can usually be brought under the Limitation Act 1980, and lets the Company show what work it did and what advice it gave. Files may be kept for longer where the SIRO is satisfied there is a continuing business need. Client confidentiality continues to apply to them.

4. Retention Schedule

4.1 The Company keeps the following records for the periods shown. Periods run from the date shown, or from the end of the year in which the record was created if no date is given.

Record	Keep for	Reason or source
Accounting records, invoices and VAT records	6 years after the end of the financial year	HMRC and the Companies Act 2006
Payroll, PAYE, National Insurance, statutory sick pay and family leave pay records	6 years after the end of the tax year	HMRC requires at least 3 years; 6 years covers tax enquiries
Pension and auto-enrolment records	6 years	The Pensions Regulator
Employee personnel files, contracts and appraisals	6 years after employment ends	Time limit for most legal claims
Right to work checks	Length of employment plus 2 years	Home Office guidance
DBS checks	Record of date, outcome and reference only; certificate not kept	DBS Code of Practice
Unsuccessful job applications	6 months after the decision	Time to respond to any discrimination claim
Working time and holiday records	2 years	Working Time Regulations 1998
Accident book and RIDDOR reports	3 years after the entry	RIDDOR 2013
Associate consultant contracts, CVs, NDAs, IR35 status records and timesheets	6 years after the engagement ends	Contract and tax claims
Client files: contracts, proposals and correspondence	15 years after the contract ends, or longer if the SIRO approves a business need	Limitation Act 1980 (15-year limit for negligence claims)
Personal data held on a client's behalf, including any patient data	Until the end of the engagement, then returned or deleted	Client contract and Part 3 of this Policy
Client files: working papers, final reports and deliverables	15 years after the engagement ends, or longer if the SIRO approves a business need	Evidence of work and advice; negligence and professional indemnity claims
Successful tender documents	Life of the contract plus 6 years	Contract and audit
Unsuccessful tender documents	3 years after the outcome	Business need
Supplier records	6 years after the last transaction	Contract and tax claims

Record	Keep for	Reason or source
Marketing contacts	Until the person opts out, or 2 years without contact	UK GDPR and PECR. Opt-outs are kept on a suppression list
Board minutes and statutory registers	Minutes 10 years; registers permanently	Companies Act 2006
Insurance policies and certificates	Permanently	Claims can arise many years later
Subject access requests and data protection complaints	2 years after closure	ICO expectations and evidence of response
Whistleblowing records	6 years after the case is closed	Whistleblowing Policy; time limit for legal claims
Data breach log and Data Protection Impact Assessments	6 years	Accountability under UK GDPR
Hospitality and Gifts, Donation and Sponsorship, and Conflicts of Interest Registers	6 years	Anti-Bribery and Corruption Policy
Training records	6 years after the person leaves	DSPT and ISO 9001 evidence
AI use log	3 years	Generative AI Usage Policy
ISO 9001 and ISO 14001 records, including internal audits	At least 3 years	Certification cycle

5. Reviewing Retention Periods

5.1 When setting or reviewing a retention period, the Company considers the purpose of the record, the law, client and framework requirements, the risk of a claim, and the rights of the people the record is about.

5.2 Where no fixed period can be set, the record will be reviewed at least once a year against those criteria.

5.3 Records must not be destroyed while they are needed for a legal claim, an investigation, an audit or a request from an individual (a “legal hold”), even if the retention period has ended. The SIRO decides when a legal hold applies and when it ends.

5.4 The Company’s general rule is to delete records when their retention period ends. A record may be kept for longer only where there is a clear reason, such as a legal hold, a possible complaint or claim, or a client, framework or regulator requirement. The SIRO decides whether there is such a reason. Personal data is never kept just in case it might be useful.

6. Secure Disposal

6.1 When a retention period ends, records are disposed of securely:

- electronic records are deleted from Company systems, and drop out of backups within the backup cycle managed by the IT Manager;
- paper records are cross-cut shredded or placed in an approved confidential waste service; and

- Company devices are securely wiped by the IT Manager before reuse or disposal.

6.2 Where a contractor shreds paper records or disposes of devices, the Company keeps any certificate of destruction they provide.

7. Individuals' Rights

7.1 People can ask the Company to delete their personal data before the end of its retention period. Requests are handled by the Data Protection Officer, as set out in the Data Protection Policy Statement. Records are deleted unless the Company has a legal reason to keep them, in which case the person is told why.

8. Roles and Responsibilities

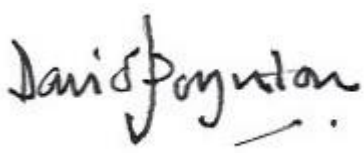
Role	Responsibility
SIRO and Information Governance Lead – John Griffiths, Managing Director	Owns this Policy. Decides on legal holds and any change to retention periods.
Data Protection Officer – Peter Case-Upton	Advises on retention periods and oversees compliance with this Policy.
Policy Administrator – Dawn Bond, Business Manager	Keeps this Schedule up to date, and runs the yearly review of records.
IT Manager – Rhys Page, RHP Ltd	Manages backups, secure deletion and the wiping of devices.
Engagement leads	Return or delete client data at the end of each engagement.
All associated persons	Keep records only in Company systems and follow this Schedule.

9. Annual Review and Related Documents

9.1 Each year, after the financial year end, the Policy Administrator arranges a review of records held against this Schedule and the secure disposal of anything no longer needed.

9.2 This Policy should be read with the Data Protection Policy Statement, the Information Governance Policy Suite (Version 08), including Records Management, Risk and Business Resilience, and the Generative AI Usage Policy. It will be reviewed every 12 months, or sooner if the law, a client requirement or the Company's work changes.

This Policy has been approved and authorised by:

Name:	David Poynton	**Position:**	Chairman
Date:	29th October 2027	**Signature:**	
Issue:	Issue 3 (replaces Issue 2, 26 May 2023)	**Next review:**	October 2027