Data Protection Policy Statement – October 2026

1. Purpose and Scope

1.1 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"), handles personal data about its employees, associates, clients, suppliers and others. In its work for NHS and other public sector clients, it may also handle information about patients, staff and services. The Company takes this responsibility seriously.

1.2 This Statement sets out the Company's commitments on data protection. The detailed rules and procedures are in the Company's Information Governance Policy Suite, in particular **Data Protection, Privacy and Confidentiality (Version 08, February 2026)**, which is the Company's full Data Protection Policy.

1.3 This Statement applies to everyone who works for or on behalf of the Company: directors, employees, associate consultants, contractors and agents ("associated persons").

2. The Law We Follow

2.1 The Company complies with the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003, each as amended, including by the Data (Use and Access) Act 2025. It also follows the common law duty of confidentiality, the Caldicott Principles and the NHS Data Security and Protection Toolkit, and the equivalent data protection laws of Jersey and Gibraltar when working there.

2.2 The Company is registered with the Information Commissioner's Office (ICO) as a data controller, registration number ZA344161.

3. Roles and Responsibilities

Role	Responsibility
Senior Information Risk Owner (SIRO) and Information Governance Lead – John Griffiths, Managing Director	Owns this Statement and the Information Governance Policy Suite. Makes sure the Company meets data protection and information security requirements.
Caldicott Guardian – Jill Griffiths, Director	Responsible for the confidentiality of person-identifiable information, including patient information.
Data Protection Officer – Peter Case-Upton (peter@pcu.co.uk)	Advises on data protection, oversees Data Protection Impact Assessments, handles requests from individuals and advises on any data breach.
IT Manager – Rhys Page, RHP Ltd	Sets up and secures the Company's systems, accounts and devices.
Policy Administrator – Dawn Bond, Business Manager	Makes sure marketing consent is in place and opt-outs are respected. Approves any software before it is installed on a Company device, advised by the IT Manager. Keeps training records and the breach and complaints logs.
All associated persons	Follow this Statement and the Policy Suite, complete training, and report any concern or breach straight away.

4. Our Commitments

4.1 The Company will make sure that personal data is:

- used lawfully, fairly and openly, with privacy notices explaining what we do and why;
- collected only for clear, specific purposes and not used for anything incompatible with them;
- limited to what is needed, and anonymised or pseudonymised wherever possible;
- kept accurate and up to date;
- kept no longer than necessary, in line with the Company's records retention schedule; and
- kept secure, using the Company's Microsoft 365 and SharePoint systems, multi-factor authentication, encryption and Company-managed devices, backed by our Cyber Essentials Plus certification.

4.2 The Company records what personal data it holds in its Information Asset Register, carries out a Data Protection Impact Assessment before any new processing likely to pose a high risk, and builds privacy into new systems and projects from the start.

5. When We Work for Clients

5.1 In much of our NHS and public sector work, the client is the controller and the Company acts as its processor (or as a sub-processor). We act only on the client's written instructions, under a data processing agreement, and follow the client's information governance requirements, including the National Data Opt-Out where it applies.

5.2 The Company does not handle patient-identifiable data unless the client's contract requires it and the right safeguards are in place. Wherever possible, we work with anonymised or summary data.

5.3 Associate consultants are bound by the same data protection terms through their consultancy agreements, and must use Company accounts and systems for all client work, saving any working copies to SharePoint at least daily.

6. Individuals' Rights

6.1 Individuals have the right to be informed, to access their data, and to have it corrected, erased or restricted. They also have the right to data portability, the right to object, and rights relating to automated decision-making.

6.2 A request can be made in any form – in writing, by email or verbally – to anyone at the Company. It must be passed to the Data Protection Officer the same day. The Company will carry out a reasonable and proportionate search and respond within one month, or within three months for complex requests, telling the person if more time is needed. There is normally no fee.

7. Complaints

7.1 Anyone who is unhappy with how the Company has handled their personal data can complain to the Data Protection Officer by email, by post or through the Company's website. The Company will acknowledge the complaint within 30 days, look into it without undue delay, and explain the outcome in plain language.

7.2 Anyone who remains unhappy can complain to the Information Commissioner's Office at ico.org.uk or on 0303 123 1113.

8. Data Breaches

8.1 Any actual or suspected data breach must be reported to the Data Protection Officer and the SIRO the same day. All breaches are recorded in the breach log.

8.2 Where a breach is likely to put people at risk, the ICO will be told within 72 hours. Where the risk is high, the people affected will be told without undue delay. Where the Company is acting for a client, the client will be told immediately, and in any case within 24 hours, or sooner if the client's contract requires.

9. Sharing and International Transfers

9.1 Personal data is shared only where it is lawful and necessary, and under a written agreement where appropriate.

9.2 Personal data is transferred outside the United Kingdom only to countries the UK recognises as having adequate protection, or with approved safeguards such as the International Data Transfer Agreement. Before any new system or AI tool is used, the IT Manager checks and records where it stores data.

10. Use of Artificial Intelligence

10.1 AI tools are used in line with the Company's Generative AI Usage Policy. No patient-identifiable data, health information about an identifiable person or HR information about an identifiable employee may be entered into any AI tool unless the client's contract allows it, a Data Protection Impact Assessment has been completed and the SIRO has given written approval.

11. Marketing

11.1 The Company sends marketing only where the law allows, gives every recipient an easy way to opt out, and respects their choice straight away. The Policy Administrator is responsible for checking consent and keeping opt-out records up to date.

12. Training

12.1 All associated persons complete data security and information governance training at induction and at least once a year, as the NHS Data Security and Protection Toolkit requires. The Policy Administrator keeps a record of who has completed it.

13. Related Documents and Review

13.1 This Statement should be read with the Company's Information Governance Policy Suite (Version 08), including Data Protection, Privacy and Confidentiality; the Information Security and IT Usage Framework; the Information Technology Policies; and Records Management, Risk and Business Resilience. It should also be read with the Generative AI Usage Policy and the Company's Privacy Notice.

13.2 This Statement is owned by the SIRO and will be reviewed every 12 months, or sooner if the law, a client requirement or the Company's work changes.

This Statement has been approved and authorised by:

Name:	David Poynton	**Position:**	Chairman
Date:	29th October 2026	**Signature:**	
Issue:	Issue 3 (replaces Data Protection Policy Issue 2, 26 May 2023)	**Next review:**	October 2027