Employee Data Protection Policy – October 2026

1. Purpose and Scope

1.1 This Policy explains how 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"), collects, uses and protects personal information about the people who work for it ("staff").

1.2 It covers current and former employees, job applicants and associate consultants, as individuals. The Company's general rules on data protection are in the Data Protection Policy Statement and the Information Governance Policy Suite (Version 08). This Policy adds the rules that apply specifically to staff information.

1.3 This Policy also serves as the Company's privacy notice for staff. Every member of staff receives a copy when they join and whenever it changes.

2. Who Is Responsible

2.1 The Company is the controller of staff information. Questions about this Policy, or about how your information is used, should go to the Data Protection Officer, Peter Case-Upton (peter@pcu.co.uk).

Role	Responsibility
Managing Director – John Griffiths (SIRO and Information Governance Lead)	Owns this Policy. Has access to health, disciplinary and grievance records, and approves any monitoring under Part 7.
Data Protection Officer – Peter Case-Upton	Advises on staff data protection, handles requests from staff and keeps the Appropriate Policy Document (see 4.2).
Policy Administrator – Dawn Bond, Business Manager	Keeps staff, training and right to work records, and works with the payroll provider.
All staff	Keep their own details up to date, and follow this Policy when handling other people's information.

3. What Information We Hold and Why

3.1 The law requires the Company to have a lawful reason (a "lawful basis") for using personal information. The table below shows what staff information the Company holds, why, and on what basis.

Information	Examples	Why we use it	Lawful basis
Identity and contact details	Name, address, phone, email, date of birth, National Insurance number, emergency contacts	To employ or engage you, and to contact someone in an emergency	Contract; legitimate interests (emergency contacts)
Recruitment	CVs, application forms, interview notes, references	To decide whom to appoint	Steps before a contract; legitimate interests
Right to work	Passport or visa copies, share codes	To prevent illegal working	Legal obligation

Information	Examples	Why we use it	Lawful basis
Pay and benefits	Salary, bank details, tax code, pension, expenses, statutory sick and family leave pay	To pay you, deduct tax and run pensions	Contract; legal obligation
Employment records	Contract, holiday, absence, appraisals, training, disciplinary and grievance records	To manage employment fairly and lawfully	Contract; legal obligation; legitimate interests
Health	Sickness absence, fit notes, occupational health advice, reasonable adjustments	To meet health and safety, sick pay and equality duties	Legal obligation, with the employment condition for special category data
Equality monitoring (voluntary)	Sex, ethnicity, religion, disability, sexual orientation, age	To check that the Company treats people fairly	Equality of opportunity condition; voluntary and reported anonymously
Vetting checks	DBS checks and professional registration, where a client requires them	To meet client contract requirements	Legal obligation or legitimate interests, with a Schedule 1 condition for criminal offence data
Associate business details	Company details, insurance, IR35 status records, timesheets	To engage and pay associates and meet tax rules	Contract; legal obligation
Bid and profile information	CVs in the Company template, short biographies, photographs	To win and deliver work for clients	Legitimate interests; consent for photographs
IT and security records	Microsoft 365 sign-in and audit logs, device records	To keep systems and data secure	Legitimate interests; legal obligation

4. Special Category and Criminal Offence Information

4.1 Health, ethnicity, religion, sexual orientation and trade union information is “special category” data and needs extra protection. The Company uses it only where necessary to meet its duties under employment, social security and social protection law, for occupational health, or for equality monitoring, as allowed by Article 9 of the UK GDPR and Schedule 1 of the Data Protection Act 2018. The Company does not rely on staff consent for these purposes, because staff may not feel free to refuse.

4.2 As the Data Protection Act 2018 requires, the Company keeps an Appropriate Policy Document explaining how it protects special category and criminal offence information. The Data Protection Officer keeps it up to date.

4.3 **Health information** is kept to the minimum needed. The Company records sickness absence and fit notes, and holds medical details only where needed to make reasonable adjustments or act on occupational health advice. Access is limited to the Managing Director and, for sick pay only, the payroll provider. Staff do not have to give medical details that are not needed for these purposes.

4.4 **Criminal offence information.** DBS checks are carried out only where a client contract requires them for the role. The Company records the date, outcome and reference number, but does not keep the certificate.

4.5 **Equality monitoring** is voluntary. Information is kept separately from personnel files and reported only in anonymous form.

5. Who We Share Staff Information With

5.1 Staff information is shared only where necessary, and never sold. It may be shared with:

- the Company's payroll provider, accountants and pension provider;
- HMRC and other public bodies, where the law requires;
- the Company's insurers and IT provider (RHP Ltd);
- clients and framework buyers, for example CVs in tenders or confirmation that vetting checks have been completed; and
- anyone you have asked us to give a reference to.

5.2 Staff information is held in the Company's Microsoft 365 systems. Any transfer outside the United Kingdom follows the rules in the Data Protection Policy Statement.

6. CVs, Profiles and Bids

6.1 The Company uses a standard CV template for all staff. CVs and biographies contain only work-related information. Home addresses, dates of birth and personal details are not included, and photographs are used only with the person's agreement.

6.2 Staff can check their CV before it is sent to a client. Clients and framework buyers receive CVs for evaluating bids and delivering work only.

7. Monitoring

7.1 The Company does not routinely monitor the content of staff emails, calls or messages. It does keep the security and audit logs needed to protect its systems, as its Cyber Essentials Plus certification requires.

7.2 Any other monitoring will take place only where it is necessary and proportionate, after a Data Protection Impact Assessment, and with staff told in advance. Covert monitoring will be used only where there is a reasonable suspicion of criminal activity or serious misconduct, and only with the approval of the Managing Director and advice from the Data Protection Officer.

7.3 AI note-taking and meeting recording may be used only in line with the Generative AI Usage Policy, with everyone present told and in agreement at the start.

8. Your Rights

8.1 Staff have the same rights as anyone else under data protection law, including the right to see the information held about them. Requests can be made in any form to the Data Protection Officer, and will be answered within one month. Complaints are handled as set out in the Data Protection Policy Statement, and staff can also complain to the Information Commissioner's Office.

9. Handling Other People's Information

9.1 When staff handle personal information about colleagues, clients or anyone else, they must:

- follow the Data Protection Policy Statement and complete annual data security training;
- use only Company accounts, systems and devices, never personal devices or personal accounts;
- never enter patient-identifiable data or HR information about an identifiable person into an AI tool, except as the Generative AI Usage Policy allows; and
- report any actual or suspected data breach to the Data Protection Officer and the SIRO the same day.

10. How Long We Keep Staff Information

10.1 Staff information is kept in line with the Data Retention Policy and Schedule. For example, personnel files are kept for 6 years after employment ends, right to work checks for the length of employment plus 2 years, and unsuccessful applications for 6 months.

11. Related Documents and Review

11.1 This Policy should be read with the Data Protection Policy Statement, the Data Retention Policy and Schedule, the Generative AI Usage Policy and the Information Governance Policy Suite (Version 08). It is owned by the Managing Director and will be reviewed every 12 months, or sooner if the law or the Company's work changes.

This Policy has been approved and authorised by:

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