Subject Access Request Policy – October 2026

1. Purpose and Scope

1.1 Everyone has the right to find out what personal information an organisation holds about them and to receive a copy of it. This is known as a subject access request (SAR). 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"), handles these requests.

1.2 It covers requests about information the Company holds as a controller, for example about employees, former employees, job applicants, associate consultants, client and supplier contacts, and website users. Part 9 explains what happens when a request relates to information the Company holds on a client's behalf.

1.3 This Policy should be read with the Data Protection Policy Statement, the Employee Data Protection Policy, the Privacy Notice and the Information Governance Policy Suite (Version 08).

2. What People Can Ask For

2.1 A person making a request is entitled to:

- confirmation of whether the Company holds personal information about them;
- a copy of that information; and
- details of why it is used, who it is shared with, how long it is kept, where it came from, and their other rights, including the right to complain to the ICO.

2.2 There is normally no charge.

3. How Requests Can Be Made

3.1 A request can be made in any form: in writing, by email, verbally or through social media. It can be made to anyone at the Company, and does not have to mention "subject access" or use a particular form. The form in Appendix A is available to help, but its use is optional.

3.2 Anyone at the Company who receives something that may be a request must pass it to the Data Protection Officer the same day.

4. Roles and Responsibilities

Role	Responsibility
Data Protection Officer – Peter Case-Upton (peter@pcu.co.uk)	Handles all requests, decides what is disclosed or withheld, and sends the response.
SIRO and Information Governance Lead – John Griffiths, Managing Director	Owns this Policy and makes sure requests are dealt with properly and on time.
Caldicott Guardian – Jill Griffiths, Director	Is consulted where a request involves health information or client patient data.
Policy Administrator – Dawn Bond, Business Manager	Logs requests and coordinates searches across the Company's systems.
All staff and associates	Pass requests on the same day, search their own files and mailboxes when asked, and never delete or alter information once a request has been received.

5. Checking Identity

5.1 The Company asks for proof of identity only where there is reasonable doubt about who is making the request, and asks only for what is proportionate. For a current employee, this will rarely be needed.

5.2 Where someone makes a request on another person's behalf, such as a solicitor or a relative, the Company will ask for written authority from the person the information is about.

6. Time Limits

6.1 The Company will respond without delay and within one month of receiving the request. If proof of identity or clarification is needed, the month starts once it has been received.

6.2 Where a request is complex, or the person has made several requests, the time limit can be extended by up to two further months. The person will be told within the first month, with the reasons.

7. Searching for Information

7.1 The Company carries out a reasonable and proportionate search of the places where the information is likely to be held, including Outlook, SharePoint, OneDrive and Teams (including chats and any AI meeting notes), the finance and payroll systems, and paper files.

7.2 Once a request has been received, information must not be deleted, altered or hidden to prevent its disclosure. Doing so is a criminal offence under section 173 of the Data Protection Act 2018.

8. Other People's Information and Exemptions

8.1 Information about other people will be removed or blacked out, unless they agree to its disclosure or it is reasonable to disclose it without their agreement.

8.2 Some information may be withheld where an exemption in the Data Protection Act 2018 applies, for example legal advice, management forecasts, information about negotiations with the person, or confidential references given by the Company. The Data Protection Officer decides whether an exemption applies and records the reasons.

9. Requests About Client Information

9.1 Where the Company holds information on a client's behalf, the client is responsible for responding. The Company will pass the request to the client straight away: the same working day where possible, and no later than the next working day, unless the client's contract sets a shorter time. NHS contracts usually require this to be done immediately. The Company will not respond directly unless the client's contract says so, and will help the client to search for and provide the information.

10. Responding

10.1 Responses are sent securely, normally by encrypted email or a secure SharePoint link, in a clear and commonly used format. If any information is withheld, the response explains why, unless doing so would itself reveal exempt information, and explains the right to complain.

10.2 Where a request is manifestly unfounded or excessive, for example because it is repetitive, the Company may charge a reasonable fee or refuse to respond. It will explain its reasons and the person's right to complain to the ICO.

11. Requests from the Police and Other Authorities

11.1 Requests from the police, HMRC or other authorities are not subject access requests. They are considered case by case by the Data Protection Officer under the exemptions in the Data Protection Act 2018, normally only on a written request. Only the information needed is disclosed, and the decision is recorded.

12. Other Rights

12.1 Requests to correct, delete or restrict the use of information, to object to its use, or for data portability are handled by the Data Protection Officer in the same way and within the same time limits.

13. Complaints

13.1 Complaints about how a request has been handled are dealt with as set out in the Data Protection Policy Statement. They will be acknowledged within 30 days. Anyone who remains unhappy can complain to the ICO at ico.org.uk or on 0303 123 1113.

14. Request Log, Training and Review

14.1 All requests are recorded in the request log, showing the date received, the due date, the steps taken, what was disclosed or withheld and why, and the date of response. Entries are kept for two years after closure, in line with the Data Retention Policy and Schedule. The Managing Director reviews the log as part of the annual management review.

14.2 All staff are told about this Policy at induction and in annual data protection training. This Policy will be reviewed every 12 months, or sooner if the law 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

Appendix A – Subject Access Request Form

You do not have to use this form, but it helps us find your information quickly. Please send it to our Data Protection Officer, Peter Case-Upton, at peter@pcu.co.uk, or by post to In-Form Solutions Ltd, Lichfield Business Hub – GF08, District Council House, Frog Lane, Lichfield, Staffordshire WS13 6YY.

1. Your details			
Full name		**Any previous names**	
Address			
Email		**Phone**	
2. Your connection with the Company			
☐ Employee ☐ Former employee ☐ Job applicant ☐ Associate consultant ☐ Client or supplier contact ☐ Website user ☐ Other (please say)			
Dates, if relevant (for example, dates of employment)			
3. What information would you like?			
Please tell us anything that will help us find it, such as dates, people, projects or types of record. You can ask for all the information we hold about you.			
4. How would you like to receive it?			
☐ Secure email ☐ Post			
5. If you are asking on someone else's behalf			
Name of the person		**Your relationship to them**	
Please attach their written authority for us to release their information to you.			
6. Declaration			
Signature		**Date**	
For office use			
Date received		**Reference**	
Identity checked (if needed)		**Response due**	