



Nexus 360

BEYOND AMBITION → STRUCTURED GROWTH

Nexus 360

Subject Access Request (SAR) Policy

Staff Group to whom it applies:	All employees, contractors, consultants and third parties acting on behalf of Nexus 360.
How to access the document:	Nexus 360 computer systems.
Issue date:	June 2026
Version:	1.0
Date of next review:	June 2027
Developed by:	Danielle Cocksedge – Data Protection and Governance Manager – ARC Management and Consultancy Services
Approved by:	Mark Shevill – Director
Amendments/Updates: Version 1.0	New policy created for Business need.

1. Policy Statement

Nexus 360 is committed to complying with its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 in relation to Subject Access Requests (SARs).

All individuals (data subjects) have the right to obtain confirmation as to whether their personal data is being processed and, where applicable, access to that personal data and supplementary information.

A Subject Access Request (SAR) is the exercise of the Right of Access, allowing individuals to request copies of personal data held about them by Nexus 360.

Personal data is any information relating to an identified or identifiable natural person, such as name, email address, contact details or identifiers.

The purpose of providing access is to enable individuals to understand how their data is being used and to verify the lawfulness of processing.

2. Purpose

The purpose of this policy is to ensure that Nexus 360 handles Subject Access Requests in a consistent, lawful and timely manner.

The objectives are to:

- Ensure compliance with UK GDPR requirements
- Enable individuals to exercise their rights effectively
- Respond to requests within statutory timeframes
- Ensure data is handled securely and appropriately
- Maintain accurate records of SAR handling
- Protect the rights and freedoms of third parties

3. Scope

This policy applies to:

- Directors
- Employees
- Contractors
- Consultants
- Temporary staff
- Agency workers
- Third-party suppliers
- Anyone acting on behalf of Nexus 360

This policy applies to all personal data held by Nexus 360 in both electronic and physical formats.

4. Definition of a Subject Access Request (SAR)

A Subject Access Request is any request from an individual (or their authorised representative) asking for:

- Confirmation that personal data is being processed
- Access to their personal data
- Supplementary information relating to that data

Requests can be made verbally, in writing or electronically.

5. Fees

Nexus 360 will not charge a fee for responding to a SAR unless the request is:

- Manifestly unfounded, or
- Excessive

In such cases, a reasonable fee may be charged based on administrative costs.

Postage or duplication costs may only be charged where requests are repeated or excessive.

6. Timeframes for Response

Nexus 360 will respond to all SARs without undue delay and within one calendar month of receipt.

Where a request is complex or involves multiple requests, the response period may be extended by up to two additional months.

Where an extension is required:

- The individual will be informed within one month
- The reason for the delay will be clearly explained

7. Handling Subject Access Requests

When a SAR is received, staff must:

- Verify the identity of the requester
- Confirm whether a third party has authority to act
- Clarify the scope of the request where necessary
- Identify relevant systems and records
- Escalate the request to a Director immediately

Where appropriate, staff should clarify the scope with the requester to ensure the correct information is provided efficiently.

All SARs must include both electronic and paper records where applicable, but only where they contain personal data.

8. Third-Party Requests

Where a SAR is submitted by a third party (e.g. solicitor or representative):

- Written consent must be provided

- Authority must be verified before processing
- The individual may be contacted directly to confirm consent

No disclosure will be made without appropriate authorisation.

9. Verification of Identity

Nexus 360 must take reasonable steps to verify the identity of all requesters.

This may include:

- Requesting photographic identification
- Verifying email addresses or contact details
- Confirming authority of third-party representatives

Failure to verify identity may result in refusal of disclosure until confirmation is received.

10. Responding to Requests

When responding to a SAR, Nexus 360 will:

- Gather all relevant personal data
- Redact third-party personal data where required
- Apply relevant exemptions where applicable
- Ensure information is provided securely
- Confirm safe receipt of information

Delivery methods may include:

- Secure email (password protected)
- Tracked postal delivery
- Secure collection (with ID verification)
- Passwords must always be sent separately from the document.

11. Redaction and Exemptions

Nexus 360 may withhold or redact information where:

- It contains personal data of third parties without consent
- Disclosure would adversely affect the rights and freedoms of others
- Information is subject to legal privilege or court restrictions
- Disclosure is restricted by law

Redactions must be applied carefully and recorded.

12. Repeated or Excessive Requests

Where identical or similar information has already been provided:

- A reasonable administrative fee may be charged, or
- The request may be refused if deemed excessive

Nexus 360 must be able to justify any refusal or fee applied.

13. Data Protection Officer (DPO) Involvement

The Outsourced Data Protection Officer (DPO) will be involved in:

- Complex SARs
- Requests involving high-risk personal data
- Disputes relating to disclosure
- Requests involving potential breaches of UK GDPR

The DPO will:

- Provide compliance guidance
- Review redactions and exemptions
- Support breach assessment where applicable
- Ensure regulatory compliance is maintained

15. Record Keeping

Nexus 360 will maintain records of:

- All SAR requests received
- Actions taken
- Response dates
- Redactions applied
- Communications with requesters

Records will be stored securely and in accordance with data protection requirements.