



DATA SUBJECT ACCESS REQUESTS (DSAR) POLICY

SNAPS YORKSHIRE CIO

July 2026

Purpose, Scope and Legal Framework

This policy explains how SNAPS Yorkshire CIO handles Data Subject Access Requests, known as DSARs or SARs, and data protection complaints. It applies to all personal data processed by SNAPS and to requests or complaints received in writing, by email, verbally, through social media, in person or through any other route. The policy reflects SNAPS' obligations under UK GDPR, the Data Protection Act 2018, relevant ICO guidance and the Data (Use and Access) Act 2025 requirements for data protection complaints.

Recognising a DSAR

A DSAR is a request from someone asking for access to their own personal data. They do not have to use the words "DSAR", "SAR" or "right of access". Examples include: "Please send me all information you hold about me", "I want to see my file", or "What information do you hold about my child?"

Responsibilities

Any employee, volunteer, contractor or trustee who receives a possible DSAR or data protection complaint must forward it immediately to the Chief Executive / Data Protection Lead. No one should delete, alter or withhold information because a DSAR or complaint has been received.

Handling a DSAR

SNAPS will confirm receipt of a DSAR as soon as reasonable possible and respond in full to a DSAR without undue delay and within one month of receipt. The deadline normally starts on the day the request is received. Where SNAPS reasonably needs clarification to understand the request, or needs to confirm the requester's identity or authority, the response period may be paused until the necessary information is received. The deadline may be extended by up to two further months if the request is complex or several requests have been made. If an extension is needed, SNAPS will tell the individual within one month and explain why.

DSAR process

SNAPS will use the following process for handling DSARs:

1. Log the request and response deadline.



2. Confirm identity where needed, especially for sensitive information, children's information, employee records or requests made by a representative.
3. Clarify unclear or very broad requests where this is reasonably required, and record when the response deadline is paused and restarted.
4. Carry out reasonable and proportionate searches of relevant records, including emails, electronic files, paper records, HR records, case notes and databases.
5. Review information before disclosure, including third-party, confidential or safeguarding information.
6. Redact or withhold information where lawful, record the reason and ensure any refusal or partial refusal is explained clearly.
7. Respond securely and keep a record of what was disclosed.
8. If the requester is dissatisfied with the response, explain how they can raise a data protection complaint with SNAPS and how they may contact the Information Commissioner's Office if the matter remains unresolved.

Refusing Requests, Fees and Exemptions

SNAPS will not refuse a DSAR simply because it is inconvenient or time-consuming. However, SNAPS may refuse to comply with a request, or charge a reasonable fee, where the request is manifestly unfounded or excessive. Any decision to refuse or charge a fee must be made case by case, approved by the Chief Executive / Data Protection Lead, documented clearly and explained to the requester.

Before disclosing information, SNAPS will consider whether any exemptions, restrictions or redactions apply. This may include information about other people, safeguarding concerns, legal professional privilege, confidential references, management planning, negotiations, regulatory matters or information that could cause serious harm if disclosed. SNAPS will disclose as much information as it lawfully can while protecting the rights and safety of others.

Data Protection Complaints Process

In line with the Data (Use and Access) Act 2025, SNAPS has a formal process for handling data protection complaints, including complaints about how a DSAR, data breach or other personal data matter has been handled:

1. Log the complaint, including the date received and issue raised.
2. Acknowledge receipt as soon as reasonably possible and within 30 days.
3. Investigate without undue delay, make appropriate enquiries and keep the complainant informed of progress where needed.



4. Provide an outcome without undue delay, explaining what action has been taken, what learning has been identified or why SNAPS believes it has complied with data protection law.
5. Tell the complainant that they may contact the Information Commissioner's Office if they remain dissatisfied, although the ICO will usually expect them to raise the issue with SNAPS first.

Informal Complaints and Employment Matters

Individuals do not have to use a formal complaints route. A data protection complaint may be made by email, telephone, conversation, social media, grievance, message to a manager or informal comment to any employee. DSARs and complaints linked to grievances, disciplinary matters or Employment Tribunal issues must still be treated as separate data protection matters and escalated promptly.

Children, Families and Third-Party Information

SNAPS works with children with additional needs and their families, so particular care must be taken when requests involve children's information. The Data Protection Lead will consider the child's age, understanding, communication needs, best interests, safeguarding issues and who has parental responsibility. Where a parent, carer, solicitor, advocate or other representative makes a request on behalf of someone else, SNAPS may ask for evidence of authority before disclosing information. SNAPS will not automatically disclose information that identifies another person and may redact or withhold information where lawful. Clear, plain language should be used wherever information is being provided to a child, young person or family member.

Data Breaches and Escalation

If a DSAR or complaint suggests that personal data may have been lost, shared incorrectly, accessed unlawfully or otherwise compromised, the matter must also be considered under SNAPS' Data Breach Policy. Serious, complex or high-risk matters should be escalated to the Chief Executive and, where appropriate, the trustees. If the complaint relates to the Chief Executive, it should be escalated to the Chair of Trustees.

Records, Training and Review

SNAPS will keep secure records of all DSARs and data protection complaints, including dates received, acknowledgement dates, actions taken, searches completed, decisions made, redactions applied, responses sent, complaints received and any learning identified. Employees, volunteers, contractors and trustees will be made aware of how to recognise and escalate DSARs and complaints. This policy will be reviewed annually, or sooner if legislation, ICO guidance or SNAPS' arrangements change.



Drafted: July 2026
Approved By Board: 15th July 2026
Next Review Date: July 2027