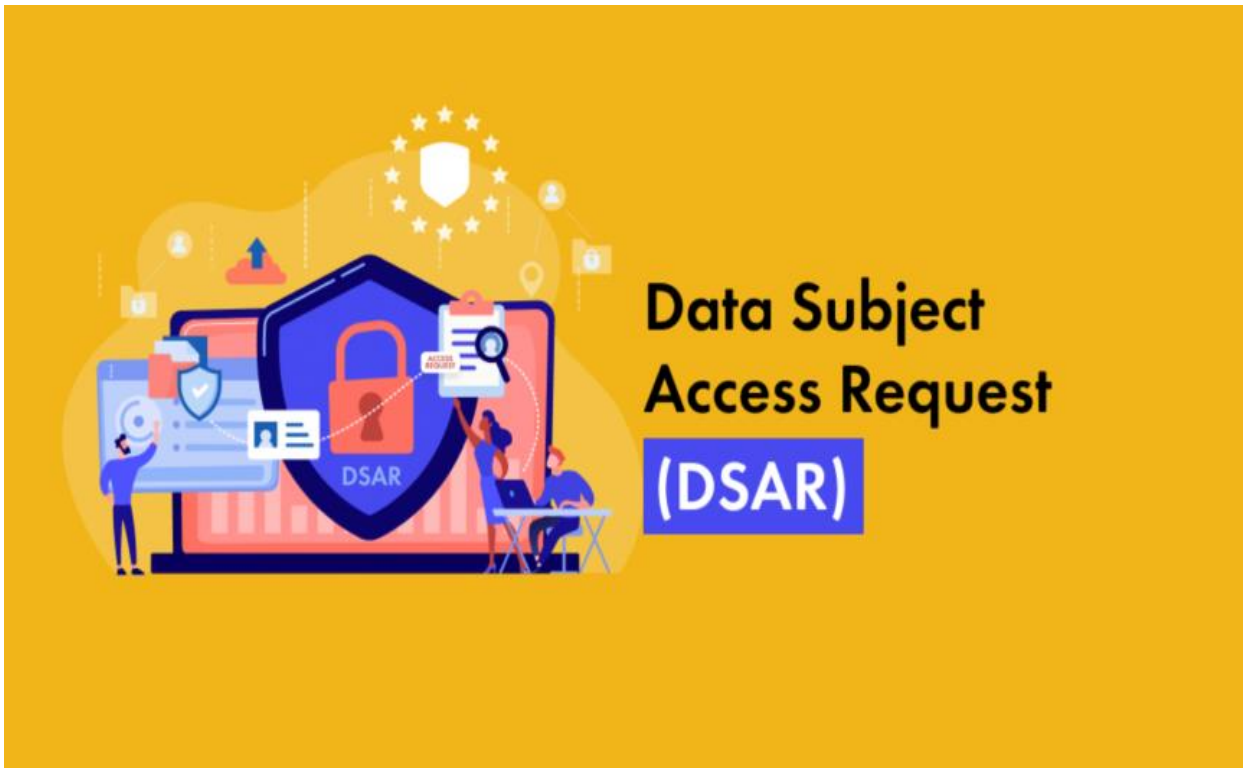
Subject Access Requests Policy



Gwybodaeth dan Reolaeth

1.0 October 2025

Subject Access Requests Policy

Document History

Name:	**Date:**	**Change:**
Helen Parry	30/09/2025	First draft
Helen Parry	06/10/2025	Approval by IG Group

Subject Access Requests Policy

1. Purpose

This policy outlines the procedures for handling Subject Access Requests (SARs) under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It ensures that individuals can exercise their right to access personal data held about them by Cyngor Gwynedd.

2. Scope

This policy applies to all employees, contractors, and third parties who process personal data on behalf of the Council. It covers all SARs received from data subjects, including employees, customers, service users, and members of the public.

3. What is a Subject Access Request?

A SAR is a request made by an individual to access personal data that an organisation holds about them. Under Article 15 of the UK GDPR, individuals have the right to:
- Confirm whether their personal data is being processed.
- Access their personal data.
- Obtain supplementary information (e.g., purposes of processing, categories of data, recipients, retention periods).

4. How to Make a SAR

SARs can be submitted via:
- Email: DPO@gwynedd.llyw.cymru
- Post: Data Protection Officer, Cyngor Gwynedd, Shirehall Street, Caernarfon, Gwynedd
- Online form: Application for your personal information

Requests do not need to mention "Subject Access Request" explicitly to be valid. Verbal requests will also be accepted.

5. Identity Verification

To protect personal data, the Council may request proof of identity before processing a SAR. Acceptable forms of ID include:
- Passport or driving licence
- Utility bill or bank statement (dated within the last 3 months)

6. Requests made on behalf of others

The Council will accept requests on behalf of others if the individual making the request has sufficient proof of authorization. Examples could include:

- Solicitor with a letter of authority
- Advocate with signed consent by the data subject
- Parent who has parental responsibility for a child

- Person who has a lasting power of attorney for a person (who may or may not have capacity)

There are two types of LPA:

- **Health and Welfare LPA** – allows the attorney to make decisions about medical care, living arrangements, and personal welfare.
- **Property and Financial Affairs LPA** – allows the attorney to manage financial matters, including accessing financial records.

For SARs:

- If the request relates to **health records**, the **Health and Welfare LPA** is required.
- If the request concerns **financial or administrative data**, the **Property and Financial Affairs LPA** is appropriate

It is for the Council to decide in all cases whether it is in the best interests of the data subject to disclose or not. Each request will be handled on a case by case basis.

7. Requests made by children

Children's Right to Access Their Data:

- Children have the same rights as adults under UK GDPR to access their personal data.
- The key consideration is whether the child is **mature enough to understand their rights**. There is no specific age set out in the legislation but it is generally accepted that parents have the right to receive information if a child is under 13. Over the age of 13, the Council must determine whether the child is sufficiently mature and competent to make a request in their own right.
- If so, the SAR should generally be responded to **directly to the child**

8. Response Time

SARs will be responded to within one calendar month of receipt. This may be extended by a further two months for complex or multiple requests. The data subject will be informed of any extension within the initial one-month period.

9. Fees

SARs are generally free of charge. However, a reasonable fee may be charged for:
- Repetitive requests
- Excessive or manifestly unfounded requests (see further below)
- Additional copies of the data

10. Data Provided

The response will include:
- A copy of the personal data
- The purposes of processing
- Categories of personal data
- Recipients or categories of recipients
- Retention periods
- Information about the data subject's rights
- Source of the data (if not collected directly)
- Details of any automated decision-making

11. Exemptions

(a) Certain data may be withheld if an exemption applies under the Data Protection Act 2018, such as:
- Legal professional privilege
  If LPP is claimed, the controller must:
    - Inform the data subject of the exemption.
    - Explain the reason.
    - Notify them of their right to complain to the ICO or apply to court.
- Confidential references
- Data involving third parties (unless consent is obtained or it is reasonable to disclose)

(b) Any information which is exempt must be appropriately redacted by trained staff using approved software. Please see redaction guidance for more details Redaction Guidance.docx

12. Vexatious or Manifestly Unfounded Requests

The Council may refuse a SAR if it is deemed manifestly unfounded or manifestly excessive.

A request is considered manifestly unfounded when:
- The individual clearly has no intention of exercising their data rights, and instead uses the request to harass, disrupt, or pressure the organisation.
- The request is malicious, such as making threats, false accusations, or targeting specific employees.
- The requester offers to withdraw the SAR in exchange for a benefit.
- The request is part of a systematic campaign to cause disruption (e.g., submitting weekly SARs with no new grounds).

A request is manifestly excessive if:
- It places an unreasonable burden on the organisation, especially if it repeats previous requests without a reasonable interval.
- It requests irrelevant or disproportionate data.
- It overlaps heavily with previous requests where no new information has emerged.

A request is not excessive simply because it covers a large volume of data. If the data is genuinely needed, the organisation must provide it unless there's a clear reason not to.

If a SAR is deemed manifestly unfounded or excessive:
- The Council may refuse to comply or charge a reasonable fee for processing.
- The decision must be made case-by-case, considering all circumstances.
- The Council must respond within one month and include a written explanation of the refusal.
- The individual must be informed of their right to complain to the Information Commissioner's Office (ICO) or pursue legal action.

13. Record Keeping

All SARs will be logged and tracked, including:
- Date received
- Identity verification status
- Date of response
- Summary of data provided
- Any exemptions applied

14. Roles and Responsibilities

- Data Protection Officer (DPO): Oversees SAR compliance and advises on complex cases.
Responsible for dealing with SAR complaints under the data protection complaints procedure
- Information Governance Team: Coordinates corporate SAR responses and liaises with relevant departments.
- Children and Adults Departments: nominated staff will process SARs
- Schools DPO: will co-ordinate and provide advice to schools
- All Staff: Must forward any SARs received to the Information Governance Team immediately.

15. Policy Review

This policy will be reviewed annually or following significant changes in legislation.

Subject Access Requests Policy

Gwybodaeth dan Reolaeth

1.0 October 2025