



Response Date:08/09/2026

2026/876 - SAR Policy

In response to your recent request for information regarding;

Please provide me with your subject access policy

Please find attached.

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST
UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 04/09/2026

Pencadlys yr Heddlu,
Glan-y-Don, Bae Colwyn LL29 8AW
www.heddlugogleddcymru.police.uk

Police Headquarters,
Glan-y-Don, Colwyn Bay LL29 8AW
www.northwales.police.uk

Yn gwneud Gogledd Cymru'r lle mwyaf diogel i fyw, gweithio ac ymweld yn y DU
Making North Wales the safest place to live, work and visit in the UK



**HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE**

Data Protection Rights Procedure

Governance:	Digital, Data and Technology (DDaT)		
Document Type:	Procedure		
Policy Owner:	Head of Information Assurance		
Department:	Information Assurance		
Policy Writer:	Data Protection & Information Assistant		
Policy Number:		Version:	1.2
Effective Date:			
Recommended Review Date:			

POLICY

CHANGE HISTORY				
Version No	Author	Changes	Ratification	Date
1.0	DP & Info Assistant	Document creation		13/07/26
1.1	DP & Info Assistant	Revised document based on department feedback.		18/08/26
1.2	DP & Info Assistant	Further amendments made after additional feedback received.		21/08/26

CONTENTS

1. WHY IS THIS PROCEDURE REQUIRED?	2
2. WHO SHOULD USE THIS PROCEDURE?	2
3. WHAT SHOULD I CONSIDER WHEN USING THIS PROCEDURE?	2
3.1 About the Data Protection Rights	2
3.2 Business as usual Requests	3
3.3 Requests relating to PNC	3
3.4 Supplying Privacy Notices	3
4. ROLES AND RESPONSIBILITIES	4
4.1 Information asset Owners (IAOs)	4
4.2 Employees (e.g. staff, Officers and Contractors)	4
4.3 Helpdesks	<i>Error! Bookmark not defined.</i>
4.4 Information Assurance	4
4.5 Information Rights Team	5
5. THE PROCESS	5
5.1 Who deals with Data Protection Rights	5
5.2 Receiving a Rights Request	5
5.3 Communicating with Requesters	5
5.4 Requests made on behalf of another	6
5.5 Fees	6
5.6 Timeframe	6
5.7 Complaints	6

6. DECLARATION & LEGALITIES..... 8**1. WHY IS THIS PROCEDURE REQUIRED?**

- 1.1 This procedure provides guidance and a process to promote compliance with the Data Protection Rights provided by the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA) and Data Use and Access Act 2025 (DUAA)
- 1.2 This procedure is primarily aimed at the Information Rights Officers within Information Assurance as they are responsible for responding to information rights requests. However, all employees must be able to recognise a request and know where to direct them. They must also know how to provide privacy details to individuals directly.
- 1.3 Knowledge of this procedure will enable all individuals working for, or on behalf of, North Wales Police to meet their responsibilities.

2. WHO SHOULD USE THIS PROCEDURE?

- 2.1 The procedure applies to all NWP officers and staff, and Office of the Police and Crime Commissioner (OPCC) staff. Any reference to staff hereafter will include NWP and OPCC staff.

3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY?**3.1 About the Data Protection Rights**

- 3.1.1 The UK GDPR and DPA set out the following rights to individuals:

- To be told how their information is used by the organisation (a **privacy notice**);
- To have **access** to their information (a Subject Access/Right of Access request)
- To have inaccurate information **rectified**;

- 3.1.2 Where appropriate, have their information **erased**;

3.2 Where appropriate, **restrict** the organisation's access to their information;

3.3 Not to be subject to **automated decisions** which can have significant or legal effects;

- 3.4 To be able to make a complaint to the organisation if they consider there is an infringement of data protection law.

3.5 In addition to the above, the UK GDPR sets out two additional Rights. These are only applicable to non-law enforcement processes;

- 3.5.1 To object to their information being used for direct marketing purposes or where the lawful basis 'Legitimate Interests' or 'Public Task' is relied on to use their information.

3.6 To have information sent to other organisations (data portability). This is typically for non-policing organisations such as energy providers (to support new quotes). It is rare that this right will apply to this organisation, but where it does, it is unlikely to be requested.

3.7 Business as usual requests

3.7.1 This procedure does not supersede any other existing legal disclosure frameworks or established disclosure processes which are already undertaken by the Force. This means there are many instances when requests for personal information are dealt with as business as usual, rather than via Information Assurance. For example;

- Staff and officers can communicate requests for basic information (such as an incident or occurrence number), without directing the individual through Information Assurance. This is providing colleagues are satisfied that the person is entitled to the information and verifying details as recorded on the incident such as their name, date of birth, and the location of incident.
- Requests from current and previous employees to view their personnel files can be arranged directly with People Services (HR).
- Requests from individuals which fall under existing disclosure frameworks, such as PACE 1984, provides an entitlement to a copy of their stop and search record, and custody record etc.

3.8 Requests relating to PNC (Police National Computer)

3.8.1 The right of access and erasure relating to information held on the Police National Computer (PNC) are facilitated by the ACRO Criminal Records Office. Employees who receive such requests should direct individuals to the ACRO website: acro.police.uk

3.9 Supplying Privacy Notices

3.9.1 Privacy notices are a key transparency requirement under data protection law which provides individuals with information about how the Force uses personal data. This information is usually provided in writing.

3.9.2 The Force publishes a general privacy notice on its website which satisfies some transparency requirements. However, business areas may need to consider supplying additional dedicated notices (e.g. when data collection forms are used). They will also need to document rationale when these notices cannot be provided to individuals (e.g. where it would prejudice operational policing matters). Such rationale could be documented within departmental procedures or a Data Protection Impact Assessment (DPIA). Business areas should seek expert advice from the Data Protection Officer (Head of Information Assurance) for all privacy notices. They should also provide copies of such notices for central storage by Information Assurance.

3.9.3 Individuals who do not speak English as their first language may request a privacy notice in an alternative language. In these instances, the business area should utilise the

interpretation and translation service contracted to the Force. Some individuals may also seek reasonable adjustments under the Equality Act 2010.

4. ROLES AND RESPONSIBILITIES

4.1 Information asset Owners (IAOs)	An IAO is usually the Head of a department of business area. They are responsible for ensuring their staff understand and follow the requirements of this document. They are also responsible for ensuring their department issues dedicated privacy notices to individuals (where appropriate) and that their staff understand where individuals should be signposted to for privacy details (i.e. the general privacy notice on the force website).
4.2 Employees (e.g. staff, Officers and Contractors)	All individuals working for, or on behalf of, the Force are responsible for recognising a written or verbal Data Protection Rights request and directing them to the Information Rights Team without delay in the event a request is made directly to them. Employees will also co-operate with Information Assurance where required to supply information to the Information Rights Team. Such information must be provided promptly and in an unedited format to ensure compliance with the legal deadline and allow the Information Rights Team to consider relevant exemptions.
4.3 Information Assurance	Information Assurance will provide data protection advice and promote awareness of this procedure. Compliance with these Rights will be monitored via the following means: • Raising awareness within the Force about the existence of these Rights, including verbal requests. • Reporting on performance at relevant meetings and Boards. For example: Information Assurance meetings and escalation to Information Management Board where required. • Reviewing information about complaints raised to the Information Commissioner's Office to assess the need for further training and awareness. • Annual review of the organisation's Records of Processing Activity (RoPA) will help to identify non-compliance with these Rights. Privacy notices will also be checked via this process.

	- Advice on Data Protection Impact Assessments will ensure projects/initiatives consider compliance with data protection rights. Information Assurance will monitor progress and completion of actions, reporting to relevant management if required. - Any notable risks will also be monitored via the organisation's risk register.
4.4 Information Rights Team	The Information Rights Team will service the Data Protection Rights requests as described in this document. In doing so, they will maintain accurate logs for all Rights requests received within Information Assurance. The Team will also consult key stakeholders to seek copies of data required or where further information is needed to enable the correct decision making on disclosure. They will also correspond directly with requesters and make decisions on the disclosure of personal data.

5. THE PROCESS

5.1 Who deals with Data Protection Rights

5.1.1 The Information Rights Team within Information Assurance deal with most of the Rights listed at section 2.1. The exception includes providing privacy detail to individuals directly (see 3.4).

5.2 Receiving a Rights Request

- 5.2.1 A request may be made to anyone working for, or on behalf of the Force. Except for existing disclosure frameworks and requests from individuals who appear to be exercising their right to receive a privacy notice, all other data protection rights must be forwarded to Information Assurance via dataprotectionengs@northwales.police.uk without delay, and certainly before the end of a shift.
- 5.2.2 Where individuals exercise their rights verbally, the following additional information must be forwarded to Information Assurance; the requester's name, detail of their request, their preferred contact details and whether the recipient can confirm their identity.
- 5.2.3 Use of application forms cannot be mandated. However, the Requests Team will actively encourage the use of such forms where appropriate to gather sufficient detail.
- 5.2.4 The Force recognises the threat posed by malicious e-mails. In accordance with IT guidance, caution will be exercised where external e-mails contain links or attachments (also see 5.3.4).

5.3 Communicating with Requesters

5.3.1 The Information Rights Team will acknowledge Rights requests in writing. Telephone can be considered where it is deemed the best method to engage with the individual (e.g. when seeking clarification) but such communication should always be followed up in writing for audit trail purposes.

- 5.3.2 The Information Rights Team will aim to follow guidance issued by the Information Commissioner's Office (ICO) regarding the methods of disclosure (i.e. electronic, paper or verbal). Viewing data, instead of providing a copy, will only be considered in the rarest of occasions. An acceptable occasion may include when it is impossible to provide a physical copy due to technical reasons, and the Force can only facilitate the viewing of the data instead.
- 5.3.3 In some circumstances it may be necessary to consider whether an individual's disability impacts on their ability to make or receive a request. The Equality Act 2010 requires the Force to consider making reasonable adjustments, depending upon the needs of the individual. Alternative methods of disclosure can be considered in these circumstances to provide reasonable adjustment. However, this alternative arrangement is still subject to affording appropriate security according to the sensitivity of the information, as described above.
- 5.3.4 Where the Information Rights Team have concerns regarding the security of email attachments or hyperlinks, they will explain this concern to the applicant and alternative options for sending the attachment will be offered.

5.4 Requests made on behalf of another

- 5.4.1 Requests may be received from agents or others acting on behalf of an individual who is unable to make the request themselves – e.g. solicitors, those granted power of attorney, or partners of those with disabilities. In such circumstances, suitable written evidence must be provided to confirm that the requestor has the power to act on behalf of the individual.
- 5.4.2 A parent or guardian can exercise the right to receive a response if a young person does not have the intellectual ability to understand the nature of the request. To qualify, the parent must be acting in the best interests of the young person and provide proof of their parental responsibility. It is generally presumed that a person of 13 years of age or older will have sufficient age and maturity to exercise the right of access.

5.5 Fees

- 5.5.1 The Data Protection Rights are free of charge. Although an administrative fee is permitted in limited circumstances, it is the Force's policy to refuse the request. This ensures a consistent and fair approach irrespective of an individual's financial means. It also allows the organisation to focus its resources on requests that are neither unfounded nor excessive.

5.6 Timeframe

- 5.6.1 Unless otherwise permitted, responses will be provided within one calendar month. This can be extended by two further months in limited circumstances. Use of the extended timeframe will be based on national guidance.
- 5.6.2 Providing the identity of the requester is verified, the deadline for all rights requests will be calculated starting on the date the request is received. Where the identity of the requester isn't verified, the deadline will be calculated starting on the date the identity of the requester is confirmed. If it is not possible to calculate one calendar month because the following month is shorter (and there is no corresponding calendar date), the date for response will be the last day of the following month.
- 5.6.3 Where clarification is required, the Information Rights Team will seek this as soon as reasonably practicable. The statutory timeframe will be paused from the date clarification is requested and will resume on the date the individual provides the necessary clarification. The legal deadline will therefore be extended by the number of days for which clarification remained outstanding.

5.7 Complaints

- 5.7.1 The Information Rights team will record and manage complaints in accordance with [DP Complaints Practice Guide](#) relating to Data Protection law and escalate to managers within Information Assurance for consideration without undue delay. Subject to any reasonable adjustments, complaints or internal review request must be made in writing and individuals are encouraged to set out their representation in a coherent and structured way.
- 5.7.2 Where an internal review of a response takes place, this will be undertaken by an independent decision-maker with the team. After the internal review, the requester should be referred to the Information Assurance complaints process and the ICO for formal assessment.
- 5.7.3 Any contact from the ICO in respect of an individual's Data Protection Rights should be forwarded to the Data Protection Officer (Head of Information Assurance) who will liaise with the Regulator directly.

5.8 Rights of the Force

- 5.8.1 The Information Rights Team may require requesters to provide further information connected with a request. A consistent approach will be applied to requests made under UKGDPR and DPA:
- To provide proof of their identity;
 - Seek clarification where a request is vague, or to help locate the data;
 - To clarify what the requester requires where there is a large volume of data about the person.
- 5.8.2 The Information Rights Team may refuse or limit access to information where permitted by law or as stated in Schedule 1 of this procedure. For example:
- Where disclosure is likely to affect other people (third party data), or where disclosure is prejudicial to the policing purpose, public or national security.
 - Where a request would involve an unreasonable or disproportionate search or is manifestly unfounded or manifestly excessive.
 - Where a request concerns paper records which are unstructured and the requester refuses to provide a description of the data or it would exceed 18 hours to determine whether the data is held.
 - Where disclosure about a child is not in their best interests. For example, where parents are in dispute with one another, or where a parent is accused of an assault or sexual assault on the child etc.
- 5.9 The Information Rights Team may cease further communication with a requestor in accordance with the Unacceptable Behaviour Policy to prevent disproportionate and unreasonable correspondence. It is recognised that:
- A small number of individuals will remain dissatisfied no matter how comprehensively the Requests Team respond.
 - It can have an unhealthy impact on the applicant and employees of the Force.
 - It hinders the public receiving information rights requests within the legal deadline.
- 5.10 When ceasing correspondence, the Information Rights Team will advise the requester of this intention in writing (where possible) at the earliest stage and advise them of their right to lodge a complaint with the ICO and to seek a judicial review in relation to

data protection matters or to Professional Standards (for police complaints), as appropriate.

6. DECLARATION & LEGALITIES

- 6.1 In line with all Force policies, the overarching purpose of this document is to directly support the PCC police and crime plan objectives. Overall, the intention of this procedure is to make North Wales the safest place to live, work and visit in the UK.
- 6.2 In the writing of this procedure cognisance has been taken of the college of policing code of ethics (2024).
- 6.3 North Wales Police policies and procedures will be written in accordance with the approved corporate format and published on the Force Intranet, allowing access to staff and public, where appropriate, on the pages of the public facing Internet site under the Force publication scheme and Freedom of Information Act 2000.
- 6.4 The following main legal requirements have been identified within this procedure:
- Equality Act 2010
 - Human Rights Act 1998
 - The Welsh Language (Wales) Measure 2011 and the Welsh Language Standards for the Chief Constable
 - Data Protection Act 2018
 - Freedom of Information Act 2000
 - Health and Safety Act 1974
- 6.5 This procedure has been written giving due regard to the above legislation and has considered the risk of unfair and/or disproportionate impacts on individuals or groups (actual or perceived) and has done so via an equality impact assessment (EIA).
- 6.6 New legislative requirements or changes in Force structure may necessitate a review of this policy document.

Schedule 1

Searches and Redaction

Purpose

This guidance provides a framework for assessing large-volume requests, including when further searching, retrieval, review and redaction may become disproportionate, and how this should be managed on a case-by-case basis.

This guidance is intended to provide clarity to requesters and support staff in handling Right of Access (RoA) requests in a lawful, consistent and practical way under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

What is a Reasonable Search?

Following the changes introduced by The Data (Use and Access) Act 2025 (DUAA), Data Protection law now makes clear that a Data Subject's Right of Access only extends to that which the Force can provide based on a reasonable and proportionate search. In other words, it is not required to carry out exhaustive searches of every possible system.

North Wales Police Approach

The Force will make genuine and properly directed efforts to identify relevant personal data, but it is not required to carry out exhaustive searches of every possible system or record as that would be unreasonable or disproportionate.

In practice, staff should seek to clarify requests where the extent of disclosure is unknown, or they reasonably require further information to identify the personal data. In doing so, it will enable staff to refine the scope where possible and methodically search the systems, date ranges, keywords and contact the business areas most likely to contain relevant personal data. This approach not only enables the data subject to describe the information at the heart of their request but also supports staff to fulfil Right of Access requests efficiently, consistently and within the statutory timescales prescribed by data protection law, as amended by DUAA.

Where clarification is not provided, or the data subject continues to seek disclosure of 'all personal data', staff should consider the significance of the information to the individual before providing personal data from the principal relevant system only, for example occurrence enquiry logs from the Crime Recording System. This approach helps to avoid significant additional effort where there is limited practical value in doing so.

Where a request is excessive because the information sought can be pursued through a separate and dedicated disclosure process, staff should consider whether the request falls within the scope of the 'Manifestly Unfounded and Excessive' provisions permitted by data protection law.

Upper Limits for Excessive Effort

There may be occasions where personal data retrieved, to satisfy the terms of the applicant's request, are so vast that to view every item would be excessive. There are exemptions within Data Protection law for this scenario together with other legislation that considers levels of reasonableness.

Each request will be looked at on a case-by-case basis and engagement with the applicant must take place. The upper limit to consider and reasons for given assets are listed below. Further advice on Manifestly Unfounded and Excessive requests is available on the Information Commissioner's Office website: ICO.org.uk.

If Manifestly Unfounded and Excessive is to be cited, the applicant must be informed without undue delay and within one month of receipt of the request, setting out the reasons, along with their right to make a complaint to the ICO, to the Force, and their ability to seek to enforce this right through a judicial remedy.

Emails – 300 Messages

This limit assumes that a thorough search has been conducted and the dataset has been refined to a point that applying a further filter would risk removing the applicant's personal data.

It is measured in that preparing 5 email messages from the dataset from their initial state to being fully redacted would take 18 minutes.

Incident Recording System – 130 Incident Reports

This limit assumes that full searches have been conducted on the system and there are more than 130 incident reports to view to ascertain if the applicant's personal data is contained in them.

It is measured in that preparing 5 incident reports, including retrieval, saving to the Network Drive and redaction would take 40 minutes.

Crime Recording System – 50 Occurrence Reports

This limit assumes that full searches have been conducted on the system and there are more than 50 occurrence reports to view to ascertain if the applicant's personal data is contained in them.

It is measured in that preparing 1 occurrence report, including retrieval, saving to the Network Drive and redaction would take 22.5 minutes.

Violent & Sex Offender Register – 135 Entries/Reports

This limit assumes that the department is contacted that has access to the system and that there are more than 135 entries to view. These entries would then need to be extracted and sent to the Requests Team.

It is measured in that preparing 1 of these entries/reports, including retrieval from the department concerned, saving to the Network Drive and redaction would take around 8 minutes per entry/report.

Professional Standards Complaint Files – 360 Pages

This limit assumes that full searches have been conducted on the system, complaint files have been identified, and a page count has been made of the contents of the files located. Full viewing of this personal data would be required to identify where the applicant's personal data resides within the files. To maximise the value of the disclosure to the data subject, staff may exclude documentation that the data subject already holds. This approach helps ensure that the disclosure remains focused on the information of greatest relevance and practical benefit.

It is measured in that viewing, locating personal data, suitably marking up and 2nd verifying 1 page would take 3 minutes per page.

Whilst it may be impractical to manually conduct the page count other indicators can be used. For example, a ream of copier paper will contain 500 sheets.

It is measured in that viewing, locating personal data, suitably marking up and 2nd verifying 1 page would take 3 minutes per page.

Whilst it may be impractical to manually conduct the page count other indicators can be used. For example, a standard ream of copier paper will contain 500 sheets and a box 2500 sheets.

CCTV & Body Worn Video

Requests for footage places a disproportionate burden on the Requests Team in terms of retrieval, review and redaction, when weighed against the likely value of the entire footage to the data subject. It is measured in that identifying relevant deployed officers, viewing, locating personal data, suitably editing would take 2 hours for footage that is 1 hour in length.

It is also recognised that CCTV and Body Worn Video (BWV) is often requested to support a Professional Standards complaint, which may fall outside the core purpose of the RoA, namely to enable the data subject to understand and verify the lawfulness of the processing of their personal data.

BWV

If the applicant requests all BWV, staff will contact the data subject to clarify this to a defined number of incidents/interactions and provide dates or approximate dates plus a short description of what they want. If footage exceeds one hour, the data subject should be asked to clarify which parts of the footage they actually need, with a brief description of what the footage covers. NWP will only provide one version of BWV relating to an incident and not a numerous recordings, all showing the same incident.

If the applicant does not clarify, the Force may either:

- Disclose only a limited core section of footage, such as the arrest and a short period before and after, or
- Where the request remains too broad and resource-intensive, refuse to provide BWV on the basis that a reasonable and proportionate search cannot be carried out.

Custody CCTV

Where held, custody footage may span several hours and include multiple camera angles, reflecting the duration of an individual's detention. A request for all such footage can therefore place a disproportionate burden on the Information Rights Team, when weighed against the likely value of the entire disclosure to the data subject.

In the first instance, staff will contact the data subject to clarify the importance of the footage sought and to identify any specific incidents or timeframes of concern. This supports the data subject's ability to challenge the accuracy of recorded information. For example, where verbal exchanges are said not to have been accurately reflected on the crime recording system, or to question whether a particular process was followed, thereby assisting them in verifying the lawfulness of their detention.

Where the data subject declines to clarify the scope of the footage required, still images will be provided in the first instance. These will confirm that the data is held and can be cross-referenced to the relevant custody record within the disclosure. The data subject may then return to the Force with details of the key timeframes or incidents they wish to have considered further.

Other Footage

This category will typically apply where the force has obtained third-party CCTV as evidential material, for example town centre or retail premises footage. Such footage may, at times, be of poor quality and can be complex to review and edit, particularly where it captures fast-moving or crowded incidents such as assaults.

From a data protection perspective, this type of footage may often hold limited value for the data subject, particularly where it records general events or interactions of which they are already aware, such as being present in licensed premises, involvement in an altercation, being removed by security staff, or subsequent verbal exchanges. In addition, the data subject may also have had the opportunity to seek the footage directly from the originating organisation.

In these cases, staff will contact the data subject to clarify the significance of the footage sought and to identify any specific timeframes or incidents of concern. Unless there is a clear and specific justification for a broader disclosure, footage should normally be limited to 15 minutes per incident.

DRAFT