WILTSHIRE POLICE
FORCE PROCEDURE

Right of Access Request Procedure

(RoARs)

Date of Publication: March 2022
Version: 3.0
Next Review Date: March 2025

TABLE OF CONTENTS

PROCEDURE OVERVIEW

Section 45 of the Data Protection Act 2018 and Article 15 of the General Data Protection Regulation (to be referred to as Data Protection Legislation for the remainder of this procedure unless a specific section/article applies) gives an individual the right of access to their own personal data held by a data controller. This procedure will enable staff to identify what constitutes a Right of Access Request (RoAR) and the procedure to be followed to allow a data subject (including children) to exercise their 'Rights of Access'

GLOSSARY OF TERMS

Term	Meaning
Data Protection legislation	Section 45 of the Data Protection Act 2018 and Article 15 of the General Data Protection Regulation
ICO	Information Commissioner's Office
ROAR	Right of Access Request
ACRO	ACPO Criminal Records Office

RELATED POLICIES, PROCEDURES and OTHER DOCUMENTS

Data Protection Policy
Right of Access Code of Practice

AUTHORISED PROFESSIONAL PRACTICE AREAS ASSOCIATED WITH THIS PROCEDURE

Data Protection MoG
Information Management > Data Protection App

DATA PROTECTION ACT 2018

This procedure is compliant with the obligations placed on Wiltshire Police in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018.

FREEDOM OF INFORMATION ACT 2000

This document has been assessed as suitable for public release.

MONITORING and REVIEW

This procedure will be reviewed every three years by the FDU Disclosure Manager.

WHO TO CONTACT ABOUT THIS PROCEDURE

FDU Disclosure Manager: christopher.harwood@wiltshire.police.uk

1. RIGHTS

1.1 Rights of the Data Subject

An individual has a right to access their personal information held by a Data Controller under Data Protection legislation.

Under the legislation individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and the following supplementary information;

    - the purposes for which the data is being processed;
    - the categories of personal data concerned;
    - the recipients or categories of recipient the personal data has been disclosed to;
    - the retention period for storing the personal data or, where this is not possible, your criteria for determining how long it will be stored;
    - the existence of the data subject's right to request rectification, erasure or restriction or to object to such processing;
    - the right of the data subject to lodge a complaint with the ICO or another supervisory authority;
    - information about the source of the data, where it was not obtained directly from the individual;
    - the existence of automated decision-making (including profiling); and
    - the safeguards provided if the personal data has been transferred to a third country or international organisation.

The following supplementary information is contained in Enclosure 2 'Data Subjects Information Notice', which should be sent with all RoAR disclosures

1.2 Rights of the Data Controller

The Chief Constable (as Data Controller) may refuse or restrict access to information to:

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;(c) protect public security;
- protect national security;
- protect the rights and freedoms of others.

The Chief Constable has the right to ask that the Data Subject to provide documentation to verify their identity.

If the request is deemed 'manifestly excessive or unfounded', the Chief Constable has the right to:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond (Where a request is refused on the grounds of being manifestly excessive or unfounded the Data Subject will be advised of this).

2 PROCEDURE

2.1 Receiving a Right of Access Request

Any request from a member of the public which appears to be asking for information/records held by Wiltshire Police should be forwarded to the Force Disclosure Unit (FDU) via the Force Disclosure Unit inbox (if received via email/Social Media), through the internal mail (if received in the post) or to Ext 62005 (if received via telephone). If forwarding a hard copy paper request then the letter should be date stamped with the date the correspondence was received in Force prior to transfer. This will allow the FDU to accurately calculate the deadline for response to such requests which is 1 month (28 calendar days) from the date of receipt.

If a request is received by an individual in person either at a Custody Suite or at an Enquiry office, staff can suggest that they complete a Form 135 - Right of Access Request, alternatively staff can follow the Verbal Right of Access Request process. Completed forms should be date stamped and forwarded to the FDU via internal mail as soon as possible.

Although an individual does not have to make a written request under DPA 2018, Wiltshire Police are not obliged to supply any information to an individual until we:

a. Have enough information to complete the request
b. Have confirmed the individual's identity (see Identification for further information)

If receiving a telephone call from a member of the public asking for information held about themselves by Wiltshire Police, staff may wish to direct them to the Right of Access Request link on our website where the Data Subject can either download a copy of the From 135 and return to the FDU either via email or in hard copy through the post; or make an online request @ https://www.wiltshire.police.uk/rqo/request/ri/request-information/rso/request-information-about-yourself-or-someone-else/. This is a very straightforward process and is directed straight to the FDU. It is important to note that a Data Subject is not obliged to complete this form in order to make a valid request under this right; however, the form will assist the applicant in providing enough detail and supporting identification documents to ensure that their request becomes valid under Data Protection legislation.

As per Section 2.1 all requests made to Wiltshire Police for disclosure of information under Data Protection legislation will require identification verification before disclosure can be facilitated.

2.2 Verification of Identity

*'The controller shall use **all reasonable measures** to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests'.*

Most requests for information received by Wiltshire Police will require the applicant to provide proof of identity. ***Please note that you only require ID if you have reasonable doubts as to the identity of the data subject – for example, if a data subject has been heavily involved with PSD and there has been several email exchanges between the two parties then it will be hard to argue that you have reasonable doubts as to the data subjects identity***. Whilst the application process insists on two forms of ID (for efficiency purposes) to show name, date of birth, address and facial image, the minimum requirements to satisfy identity verification should be a document/record, which verifies the Data Subject's **name and date of birth.** For any requests relating to obtaining video or photographic records such as custody photographs or Body Worn Video footage, photographic identification must be produced. If the request is received in the post and the applicant wants a hard copy response, then confirmation/proof of address will be required.

The identity of the data subject must be validated on all occasions before disclosure of information is made to them.

This proof of identity may include:

Birth/adoption certificate
Marriage certificate
Driving licence
Medical card
Passport
Pension book/statement
Benefits statement
Insurance certificate (not schedule)
Hire purchase agreement
Or, any other official certified document.
Utility bill
Telephone/Mobile statement
Bank statement
Credit/debit card statement
Council tax bill
Rent book

Requests identifying photographs or videos will require **photographic** proof of identity–

Passport
Photo driving licence
Identity cards
Bus passes/membership cards, etc. (an additional proof of identity will also be required)

The level of checks you make may depend on the possible harm and distress that inappropriate disclosure of the information could cause to the individual concerned.

2.2 Consent for Release of Information to Third Parties

An individual can ask for information disclosure to be made to a third party acting on their behalf such as a Solicitor.

Consent of the data subject is defined as:

Any freely given, specific informed and unambiguous indication of the data subject's wishes by which he or she by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

In order to facilitate disclosure to a third party, the Data subject will need to provide explicit and specific consent at the time of making their request. This can take the form of:

I. A short statement within the request affirming that disclosure is to be made to a third party and details of that party along with the specific description of the information to which the consent relates
II. By completing Section 2 of the Form 135 available on our website or section 2 of the online form.

Identification of the Data Subject will still need to be provided (if you have reasonable doubt as to their identity).

2.3 Request Details and Sourcing Information

The Data Subject should identify the information to which he or she requires access by providing a description of this information within their request at section 2 of the online form or the form 135. Please note that there is no requirement to complete either form, however where we process large volumes of data it is best practice to engage with the data subject to identify the information they require. This can include incident or occurrence numbers or dates and times when the information is likely to have been captured.
Recital 63 states:

Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

All details provided within the Right of Access Request will be held for the purposes of facilitating disclosure in line with the Data Subjects rights of access. Copies of requests and accompanying documents will be scanned into the associated task and retained for a maximum of 36 months from the date the request is closed. This is in line with our retention schedule.

The decision maker will review the information being requested and access the appropriate computer systems in order to locate the records/information being sought. These records will then be saved in to the associated folder within 'SharePoint' for disclosure to be considered and facilitated. The decision maker will apply any redactions and restrictions on access to information as per Data Protection legislation and ***fully record*** the decisions for these on the task. This includes the redaction of third party and operationally sensitive material. It should be noted that it is **now a legislative requirement** to articulate the reasons for a decision to restrict (whether wholly or partly) the rights of a data subject.

During the course of their research, decision makers may have cause to liaise with individual Police Officers or Departments in order to locate any specified records or information falling within the scope of the Data Subject's request. The decision maker must not be impeded in this research and any records requested by the decision maker should be provided to them in order for them to consider any exemptions on disclosure. Where possible, supplying officers/staff/departments should make the decision maker aware of any areas of sensitivity, however, it is the responsibility of the decision maker to apply any appropriate exemptions on disclosure. Any exemptions placed on disclosure should be done in line with the Data Protection legislation.

Deleted Information - Information is 'deleted' when you try to permanently discard it and you have no intention of ever trying to access it again. The ICO's view is that, if you delete personal data held in electronic form by removing it (as far as possible) from your computer systems, the fact that expensive technical expertise might enable it to be recreated does not mean you must go to such efforts to respond to a Right of Access request.

The contents of emails stored on Force computer systems are a form of electronic record to which the general principles above apply. For the avoidance of doubt, **you should not regard the contents of an email as deleted merely because it has been moved to a user's 'Deleted items' folder.**

It is not acceptable to amend or delete the data if you would not otherwise have done so.
Under the DPA 2018, it is an offence to make any amendment with the intention of preventing its disclosure.

2.4 Disclosure

Under Data Protection legislation, an individual is only entitled to their own personal information, held by a data controller. The decision maker will review records located as a result of their research and will remove any information which relates to a third party, any information which is tactically sensitive or any information which falls within an exemption under the legislation. This redaction of PDF documents will be as per the Redacting Personal Data Procedure to ensure that any electronically disclosed material will not be able to be un-redacted by the recipient.

Completed disclosures will be tasked to the FDU administrator who will format the documents and return to the relevant decision maker.

Disclosure will be made via Egress. Hard copy disclosure will only be made in exceptional circumstances. If the Data Subject specifies no preference at the time of making their request, response will be made via Egress. If the decision maker is unsure of the means of communication then contact should be made with the applicant.

If the only option is hard copy disclosures, this will be sent to the applicant via special delivery to ensure safe receipt of the requested information. Such delivery method will require the applicant to be available to sign for the delivery. The cost of providing information by this method will be charged to the applicant. The minimum cost for special delivery is £6.50 (this charge increases to £7.30 for larger parcels) and this fee will be applied to all requests involving postal delivery.

Data Subjects can choose to collect their disclosure from any of the Force enquiry offices. This preference must be specified to the FDU prior to the disclosure being made. The decision maker or FDU workflow coordinator will arrange with the respective enquiry office to have the information internally sent via Egress. The Data Subject will need to show valid original identification prior to collecting the disclosure and may be required to sign a receipt to indicate that the disclosure has been collected.

A copy of the completed response will be held in the 'SharePoint' folder for a maximum of 36 months (2 years plus current year) from disclosure from the date the request is closed in line with our retention schedule.

There is no requirement to translate the information we hold into another language as the applicant has poor English comprehension skills. You are only required to send a response which can be understood by the average person. However, it is good practice to help individuals understand the information we hold about them.

Can we provide the information verbally?

If an individual asks, you can provide the response to their SAR verbally, provided that you have confirmed their identity by other means. You should keep a record of the date you responded and what information you provided. This is most likely to be appropriate if they have requested a small amount of information.

You are not obliged to provide information in this way. However, we should take a reasonable approach when considering such requests.

All applications for disclosure will be acknowledge on receipt by the FDU

Exemptions

In line with the accountability principle, you should justify and ***document*** your reasons for relying on an exemption so you can demonstrate your compliance.

What should we do if we refuse to comply with a request?

If you refuse to comply with a request you must inform the individual of:

- the reasons why;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

If you believe, a request is manifestly unfounded or excessive you must be able to demonstrate this to the individual.

Where an exemption applies, the reasons you give to an individual for not complying with a request may depend upon the particular case. In line with s45(6) of the DPA'18 there is no requirement to articulate why a disclosure has been fully or partially restricted if that, in itself, would prejudice the exemption you are relying on. However, if it is appropriate to do so, you should be transparent about your reasons for withholding information.

2.5 Timescales

Requested information should be provided immediately and at the latest, within one month of receipt of the request.

The 'clock' will not start until the FDU is in receipt of all the required information to enable it to progress the request, such as identification documents.

If the further information is not received within one month of being requested by the FDU, the request will be closed and the applicant informed in writing/email. The request can be reopened at any time upon receipt of the requested information from the Data Subject.

Where a request is overly complex and involves a large number of records to be reviewed, the deadline for compliance can be extended by the FDU up to an **additional 2 months.** (Note this refers to GDPR processing only – HR/Finance/Recruitment/PSD etc.). Where this applies, the Data Subject will be notified in writing/email within the initial one month deadline. From a customer service perspective, the data subject should be informed as soon as is practical and not within the last few days of the due date. It therefore follows that decision makers should assess applications on receipt to identify the volume of data held.

Disabled people

Some disabled people may experience communication difficulties, and may therefore have difficulty making a SAR. We have a legal duty to make reasonable adjustments if they wish to make a request.

If the request is not straightforward, you should document it in an accessible format and send it to the disabled person to confirm the details of the request.

Before responding to a SAR you should liaise with the applicant to find out how best to meet their needs. This may be by providing the response in a particular format that is accessible to the person, such as large print, audio formats, email or Braille. If an individual thinks you have failed to make a reasonable adjustment, they can make a claim under the Equality Act 2010 or the Disability Discrimination Act 1995 (NI). Further information about your legal obligations and how to make effective reasonable adjustments is available from the Equality and Human Rights Commission or from the Equality Commission for Northern Ireland.

2.6 Manifestly Unreasonable, Excessive or Unfounded Requests

If the request is deemed 'manifestly unreasonable, excessive or unfounded', The Chief Constable has the right to:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond

Data Subjects could potentially attempt to use the Subject Access process as a means to harass Police Forces with no real purpose other than to cause disruption. An example of this can be repeated requests for the same information over a short period of time (or over several years) or where the Police Force has provided the Data Subject with their personal data through an alternative disclosure mechanism e.g. pre-trial information being disclosed under CPIA and the same information being requested through a Right of Access Request.

'Excessive requests' can refer to those which would involve a substantial effort to respond to.

'Unfounded requests' are those which are clearly without basis or where the request is not made out.

Any request which asks for "all information held about me" or "all emails in which my name is mentioned" may be considered to be manifestly excessive and/or unfounded and will be rejected for further refinement from the data subject.

In the event that a request 'has the potential' to be refused by Wiltshire Police, you should discuss with the FDU PDM in the first instance for a second opinion. If required, the Data Subject should then be contacted to offer them the opportunity to refine their request or clarify the information sought. If, having advised the data subject of the need to refine their request, as it is deemed to be Manifestly Unreasonable, Excessive or Unfounded, they are still dissatisfied, then the Data Subject should be advised on their 'right of appeal' to the Information Commissioner.

2.8 Fees

The majority of Right of Access Requests will not involve a fee. Information will be provided free of charge to any individual making a Right of Access Request unless:

- The request is manifestly unreasonable, excessive or unfounded
- The request asks for a further copy of information which has already been disclosed

Any fees deemed relevant by Wiltshire Police will be based on the administrative cost of providing the information only.

In the event that Wiltshire Police deem a fee to be chargeable in response to a Right of Access Request, the Data Subject will be advised in writing by FDU within 28 days of receipt of the request. The disclosure will not be facilitated until such time as the required fee is received by Wiltshire Police.

Disclosures provided in response to initial Right of Access Requests to Wiltshire Police and which are facilitated via Egress or by the data subject collecting in person will be provided free of charge unless they are deemed to be excessive. Subsequent requests made by the same applicant for the same information within a 60 day period will attract a reasonable disbursements charge.

Data Subject requested hard copy disclosures will be sent to the applicant via special delivery to ensure safe receipt of the requested information. Such delivery method will require the applicant to be available to sign for the delivery. The cost of providing information by this method will be charged to the applicant. The minimum cost for special delivery is £6.50 (this charge increases to £7.30 for larger parcels) and this fee will be applied to all requests involving postal delivery. The fee must be paid prior to any disclosure being facilitated.

2.9 Requests for Conviction Information Held on the Police National Computer

Requests for copies of conviction records or copies of any information held on the Police National Computer (PNC) will be facilitated by ACRO Criminal Records Office and **NOT** Wiltshire Police.

Such requests should be made directly to the ACRO Criminal Records Office as per the details on their website: https://www.acro.police.uk/Subject-access

Any request for PNC records received by Wiltshire Police will be rejected and the applicant advised to redirect their request to the ACRO Criminal Records Office.

2.10 Other Means of Disclosure

Decision makers should be aware of other disclosure routes and, where appropriate, direct applicants to the correct / most appropriate disclosure regime.

Examples include:

- DBS disclosure for employment is facilitated through the Disclosure and Barring Service.
- Requests for copies of Custody Records and interview recordings under PACE are facilitated through custody.
- Victim updates in relation to on-going criminal investigations are facilitated in line with the Victims Code of Practice through Horizon.

2.11 Calls to Control Room/FDU asking for Incident/Occurrence Numbers

When a member of the public calls up for basic information such as an incident or crime number; providing you are satisfied that they are the person entitled to the information (possibly by asking them to verify basic details as recorded on the incident such as their name and date of birth, or the location of incident), it is appropriate to pass the incident number or Niche Occurrence number only.

2.12 Enforced Right of Access Requests

Certain employers and organisations such as recruitment agencies may attempt to exploit the subject access process by requiring individuals to use it to obtain a copy of their criminal convictions (or evidence that there is nothing held) as part of recruitment or continuing employment processes.

This process, known as enforced subject access, is legislated through **Part 7 section 184 of the Data Protection Act 2018**. It states it is a criminal offence for a current or prospective employer or recruitment agency to require an individual to make a Right of Access Request as a condition of employment or for the provision of goods or services. They should instead be using the existing formal criminal records check arrangements operated by the Disclosure and Barring Service, Disclosure Scotland or Access Northern Ireland.

Where a Right of Access Request is made and the applicant clearly states that the information is for employment purposes, the request will be rejected and the data subject will be redirected to the appropriate agency.

The applicant can identify whether they have been asked to seek disclosure from an agency within Part 2a of the Right of Access Request form. Positive indication will not affect the data subject's right to information under the Act and their request may continue to be processed as per the Act, however, the Information Commissioner should be notified of the request.

2.13 Right of Access Requests from Children

Children are to be afforded the same rights regarding access to their information as is given to adults as long as they are competent to do so. You must bear in mind that it is the right of the child rather than of anyone else, such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a Right of Access Request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

What matters is that the child is able to understand (in broad terms) what it means to make a Right of Access Request and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:

- the child's level of maturity and their ability to make decisions like this; (why are they requesting it)
- the nature of the personal data; (what does the data relate to and in what context is the child involved)
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;

- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

In Scotland, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. This presumption does not apply in England and Wales or in Northern Ireland, where competence is assessed depending upon the level of understanding of the child, but it does indicate an approach that will be reasonable in many cases.

The parent must provide proof of parental responsibility in these cases as well as valid identification for themselves. Disclosure will not be facilitated until we are in receipt of such documents as required to validate the requestor's identity and parental responsibilities to the child in question.

2.14 Complaints Procedure

Where an applicant is dissatisfied with how their Right of Access application has been processed they should follow the complaints procedure contained in the response letter. They have 30 days of receiving their response to register their complaint.

On receipt of a complaint the Principal Decision Maker (PDM) will conduct a review of how their application was processed, any redaction(s) that were made and the disclosure that was provided. The PDM will provide a narrative of their findings / decision, which will be communicated back to the applicant by the DM.

DOCUMENT ADMINISTRATION

Ownership:

Department Responsible: Force Disclosure Unit
Procedure Owner/Author: Keith LEWIS / Chris Harwood (Author)
Technical Author:
Senior Officer/Manager Sponsor: Head of Information Management and Assurance

Revision History:

Revision Date	Version	Summary of Changes
11.07.2018	1.0	Draft
30.07.2018	1.1	Feedback from FDU
11.02.2020	2.0	Review in light of RoAR ICO guidance
11.03.2022	3.0	Scheduled Review. New section on complaints added.

Approvals:

This document requires the following approvals:

Name & Title	Date of Approval	Version
Continuous Improvement Team		
Senior Command Team/ACC/ACO (Delete as appropriate)		
JNCC (Not required for all procedures)		

Distribution:

This document has been distributed via:

Name & Title	Date of Issue	Version
E-Brief		
Email to relevant affected Staff/Officers		
Other: *(state method here)*		

Diversity Impact Assessment:

Has a DIA been completed? If no, please indicate the date by which it will be completed. If yes, please send a copy of the DIA with the procedure.	☐ **Yes** ☐ **No** **Date**:

Consultation:

List below who you have consulted with on this procedure (incl. committees, groups, etc):

Name & Title	Date Consulted	Version

Implications of the Procedure:

Training Requirements

No additional training requirements.

IT Infrastructure

No additional IT infrastructure required.