SUBJECT ACCESS POLICY AND PROCEDURE

Document Control	
Version Number	1.0
Author (Name, Job Title)	Joanne Regan (Head of Assurance and Compliance – Gwent OPCC)
Date Approved	May 2021
Approved By	Carys Morgans (Dyfed-Powys OPCC CoS)
Date of Next Review	May 2025

Version Control			
Version	**Date**	**Amended By**	**Reason for Issue/Amendment**
1.1	*31/03/21*	*Cheryl Gayther*	*Amendment of job titles from Chief Executive to Chief of Staff, Governance Officer to Compliance and Performance Support Officer.* *References to Gwent replaced with Dyfed-Powys*
1.2	*10/05/21*	*Debby Jones/Gemma Blake*	*Amend to SAR timescale*

OFFICE OF THE POLICE AND CRIME COMMISSIONER
SUBJECT ACCESS REQUEST POLICY AND PROCEDURE

1. Introduction

Article 15 of the UK-General Data Protection Regulation (UK GDPR) provide data subjects with a right of access to the personal data which organisations hold about them, subject to certain exemptions. Requests for access to personal data are known as Subject Access Requests (SARs). A request can be made in writing (including via social media) or orally. If it is made orally, then it must be treated no differently to a written request except extra care must be taken to ensure the identity of the applicant and clarification of the type of information sought.

2. Aim

This policy clarifies the statutory rights that data subjects have over their data and the procedures in place for ensuring that their rights are consistently met. It also provides guidance to OPCC staff to assist in responding to any requests in a timely, consistent manner and in compliance with legislation.

The basis of this policy will be adopted across the four Welsh Offices of the Police and Crime Commissioner (OPCC), although altered to suit local need, in order to provide consistency to data subjects making requests across Wales.

3. Terms and Definitions

Term	Definition
Personal Data	This can be defined as information which relates to a living data subject who can be directly or indirectly identified from the data available, eg name, address, postcode, vehicle registration mark, ID number such as a National Insurance number or NHS number, payroll or collar number, location data, online identifier (IP address and cookie identifier), photographic or video image. It also includes any expression of opinion about a data subject and any indication of the intentions of the data controller or any other person in respect of that data subject.
Processing of personal data	This refers to the obtaining, recording, holding or performing any operation in any capacity relating to personal data, and applies to both manual and computerised records.
Data subject	The data subject to whom the personal information relates.

Data controller	A person or an organisation who determines the purpose for which, and manner in which, personal data is to be processed.
Data processor	Any person or organisation who processes data on behalf of the Data Controller.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, disclosure of or access to, personal data.

4. Policy and Procedure

Policy

4.1 Rights of Access

4.1.1 The right of access, commonly referred to as a SAR, gives data subjects the right to obtain a copy of their personal data. This information helps them understand how and why we are using their data and to check we are doing it lawfully.

4.1.2 Data subjects have the right to obtain the following from a controller

- Confirmation that you are processing their personal data;
- A copy of their personal data; and
- Other supplementary information

4.1.3 When responding to a SAR, in addition to a copy of their personal data held by the OPCC, the data subject also needs to be provided with:

- the purpose for the processing of their data;
- the categories of personal data concerned;
- the recipients or categories of recipient you disclose the personal data to;
- your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the Information Commissioner;
- information about the source of the data, where it was not obtained directly from the data subject;
- the existence of automated decision-making (including profiling); and
- the safeguards you provide if you transfer personal data to a third country or international organisation.

4.1.4 This information can be found in our Privacy Notice. Providing a link to the Privacy Notice in the response should be sufficient to meet the criteria above. If the data subject does not have internet access then a paper copy must be provided.

4.1.5 Should the data subject require any clarification or further information regarding how their data is used, you must refer the data subject to the Data Protection Officer (DPO).

4.2 Receiving a Subject Access Request

4.2.1 The OPCC has a SAR Form (appendix a), which is designed to gather the information which is needed to identify, communicate and locate the required data the data subject is requesting. There is no legal requirement to complete the form when submitting a request, but it is a helpful guide for both the OPCC and data subjects in clarifying who the data subject making the request is and what information they wish to receive.

4.2.2 Any request from a data subject which appears to be asking for information/records containing personal information should be date stamped and forwarded to the Compliance and Performance Support Officer. The Compliance and Performance Support Officer will then determine if the request is a SAR, that the information being requested is clear and that there is sufficient evidence to confirm the data subject's identity or whether further evidence may be needed. The request will be acknowledged, with a request for further evidence if required, and a date will be provided as to when the data subject can expect a response; this is one month starting the day the request is received. However, please note that the request will be 'on hold' if evidence of identity is required and will not be restarted until this has been received and confirmed.

4.2.3 Requests for access to personal information may also be received at police stations across Dyfed-Powys. Where this is the case, the Station Enquiry Officer should provide the OPCC SAR form to the data subject (although if the Dyfed-Powys Police form is provided, this will also be accepted). Where the subject wishes to make an oral request, the Station Enquiry Officer should verify the identity of the subject in accordance with the procedure below which is common to Dyfed-Powys Police and the Dyfed-Powys OPCC and ensure that the OPCC is made aware of the request in a timely manner. Following receipt of the information, the OPCC will be solely responsible for handling the request. Alternatively, contact details for the OPCC should be provided for a direct request to be made

4.2.4 Requests will be dealt with within the statutory time scale of one calendar month. If the request is complex, then an extension of another two months is permissible, provided that this is communicated to the individual in a timely manner within the first month.

4.3 Identification

4.3.1 In most cases, two forms of identification will need to be produced at the time of making a SAR in order for the request to be processed.

4.3.2 Identification must **not** be requested where the identity of the data subject is already known as this will be deemed unreasonable. One such example of this is where a member of staff of the OPCC makes a SAR; to require a utility bill, payslip or passport would be unreasonable, as their identity will already be known.

4.3.3 The purpose of identification is to establish the correct name, date of birth, current address and be able to check the signature on the form/letter. The OPCC may require further information in order to satisfy itself as to the identity of the data subject and will inform them of that requirement where necessary. It is important to confirm the identity of the person making the application to ensure the personal data is disclosed to the data subject and not to someone impersonating them.

4.4 Sufficient Information

4.4.1 If the data subject does not provide sufficient information as is reasonably required to locate the personal data sought, the OPCC must inform the data subject that further information is required. These steps must be taken as soon as possible after receiving an application. In most circumstances, a SAR 'for everything you hold about me' would in itself constitute insufficient information and would require further clarification. However, there may be limited occasions where the nature of the relationship between the data subject and OPCC and context of the request could make such a request sufficient.

4.4.2 When a request for clarity has been sent to a data subject the timeframe in which a response will be provided will be paused. It will only resume once clarity has been provided.

4.4.3 Where the data subject has made a request for information only partly held by the OPCC and the remainder is likely to be held by Dyfed-Powys Police, the Compliance and Performance Support Officer will make contact with the data subject and notify them that the OPCC can transfer the relevant parts of the request to Dyfed-Powys Police, or they may make a separate application to the force themselves. If the data subject elects for the latter, then they will be informed that the request will be handled by the force and that a new point of contact will be established.

4.5 Consent for Release of Information to Third Parties

4.5.1 A data subject 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.

4.5.1 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. Identification of the data subject the request is about will still need to be provided to the OPCC.

4.6 Applications made on Behalf of a Young Person

4.6.1 SAR's can be accepted from a young person where they are believed to have sufficient intellectual ability to understand the nature of the application. There is no age limit defined in Wales but in Scotland it is generally presumed that a person of twelve years of age or over will have sufficient age and maturity to exercise the right of subject access. A child should not be considered to be competent if it is evident that he or she is acting against their own best interests.

4.6.2 A parent or guardian can exercise the right and receive the reply, if the young person does not have the intellectual ability to understand the nature of the application, and the parent is thought to be acting in the best interests of the young person. At all times the person processing the SAR must record their decisions and rationale.

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

4.7 Sourcing of Information

4.7.1 Once the OPCC is in receipt of a valid request, it will be recorded and the Compliance and Performance Support Officer will conduct a search of the OPCC's electronic records, filling systems, databases and paper records that might contain the data subject's personal data. Any personal data produced from that search, relating to the data subject, will be scrutinised to ensure that the information is appropriate for disclosure. Where information is located, but elements aren't suitable for disclosure, such as personal information relating to another data subject, the Compliance and Performance Support Officer will ensure that redactions are applied appropriately. At all times, exemptions and redactions are to be recorded and the rationale noted.

4.7.2 When all information has been sourced and it becomes clear that information held by the OPCC has been provided by a different data controller (in most cases this is likely to be the police force), then the OPCC must liaise with the original data controller, informing them of the request and the information that may be released. The data controller should be asked if any of the information they have provided should be exempt and if so under what exemption and a rationale provided. The OPCC must then consider this feedback prior to making the final decision.

4.8 Disclosure of Information

4.8.1 Disclosure will be made either in hard copy or via electronic means such as email as per the request of the data subject. If no preference is specified at the time the request is made, where possible, the response will be provided via the same method as the request was made. If the request was made via social media an alternative method of disclosure will be required.

4.8.2 Emailed disclosure will be via a word or adobe document which will be password protected and sent to the data subject to the email address specified within their request. Where disclosures have been password protected, the data subject will be required to contact the OPCC in order to be provided with the password required to open the documentation. This is to protect the data subject against unauthorised access to any sensitive or confidential information being disclosed.

4.8.3 Hard copy disclosures will be sent to the data subject via Royal Mail Signed For. If an alternative method is requested by the data subject that is more costly then the OPCC is able to charge for the increased fee and the cost of any additional administrative work.

4.8.4 Alternatively, the data subject can choose to collect their disclosure from the OPCC at Police Headquarters by making a prior appointment. This appointment must take place between 9am-5pm Mon-Thu and 9am-4pm on Friday. 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.

4.9 Fees

4.9.1 The majority of SARs will not involve a fee. Information will be provided free of charge to any data subject making a SAR unless:

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

4.9.2 Those requests that are deemed chargeable will have a reasonable fee applied to cover the administrative cost of complying with the request.

4.9.3 Disclosures provided in response to initial SARs to the OPCC and which are facilitated via email or by the data subject collecting in person will be provided free of charge unless they are deemed to be excessive. Identical requests made by the same applicant will not be responded to unless reasonable time has elapsed or there is a reasonable circumstance for the request to be made but this may attract an administrative fee.

4.10 Refusing a Request – Exemptions and Manifestly Unfounded/Excessive

4.10.1 The Act clearly defines the applicable exemptions which specify the circumstances in which the OPCC can refuse to provide access to personal data. These, along with further guidance, are clearly listed on the Information Commissioner's Office website.

4.10.2 As well as the exemptions, a SAR can also be refused if it is deemed to be 'manifestly unfounded' or 'manifestly excessive'.

Manifestly Unfounded

4.10.3 A request may be manifestly unfounded if:

- the data subject clearly has no intention to exercise their right of access. For example an data subject makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
- the request is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption. For example, the data subject:
- explicitly states, in the request itself or in other communications, that they intend to cause disruption;
- makes unsubstantiated accusations against you or specific employees which are clearly prompted by malice;
- targets a particular employee against whom they have some personal grudge; or
- systematically sends different requests to you as part of a campaign, eg once a week, with the intention of causing disruption.

4.10.4 A request must be considered in the context in which it is made. If the data subject genuinely wants to exercise their rights, it is unlikely that the request could be deemed to be manifestly unfounded.

Manifestly Excessive

4.10.5 To determine if a request could be deemed to be manifestly excessive, consideration needs to be given as to whether it is clearly or obviously unreasonable. This should be based on whether the request is proportionate when balanced with the burden or costs involved in dealing with the requests.

4.10.6 This will mean taking into account all the circumstances of the request, including:

- the nature of the requested information;
- the context of the request, and the relationship with the data subject;
- whether a refusal to provide the information or even acknowledge if you hold it may cause substantive damage to the data subject;
- available resources;
- whether the request largely repeats previous requests and a reasonable interval hasn't elapsed; or
- whether it overlaps with other requests (although if it relates to a completely separate set of information it is unlikely to be excessive).

4.10.7 A request is not necessarily excessive just because the data subject requests a large amount of information.

4.10.8 Consideration should also be given to asking the data subject for more information to help locate the information they want and whether reasonable searches can be made for the information.

4.10.9 It is important to consider each request individually and for clear justifications to be recorded as to why a decision was made to use an exemption or to treat as request as being manifestly unfounded or excessive. An explanation must also be provided to the data subject to explain why the data has been withheld and the relevant exemption, unless doing so would itself disclose information which would be subject to the exemption. A record of this information will also be recorded and kept by the OPCC in an exemption register.

4.11 Responding to Subject Access Requests

4.11.1 When the information has been collated in a secure and readable format, the Compliance and Performance Manager will review the redactions, edits, exemptions and overall information and approve or reject the disclosure. Where the disclosure is rejected, the Compliance and Performance Support Officer will complete any amendments that are required and ensure that contact is maintained with the data subject in order to manage expectations. At all times, decisions made by OPCC staff will be recorded and justified when necessary.

4.11.2 When returning the SAR information, the data subject or third party will be made aware of their right to rectification, restriction of editing and of the opportunity to complain, firstly to the OPCC and then if still not satisfied to the Information Commissioner's Office.

4.12 Making a Complaint

4.12.1 Where a data subject or their third party makes a complaint about the way a SAR has been handled by the OPCC, the Compliance and Performance Support Officer shall be informed so that records may be maintained. The Chief of Staff and Monitoring Officer will carry out a review of the processes followed and ensure that the Compliance and Performance Support Officer is updated on the progress of the review. The Compliance and Performance Support Officer will ensure that the complainant is provided with a realistic and reasonable date by which they can expect to hear from the OPCC regarding their complaint.

4.12.2 The data subject will be informed of the outcome of their complaint in written format. The complaint will also contain details of the data subjects right to make a complaint to the Information Commissioner's Office.

4.13 Rectification of Incomplete or Incorrect Data

4.13.1 It is possible that upon receipt of their information, the data subject notices that the OPCC has held incomplete or inaccurate data about them. Under the Act they may seek to rectify this. The data subject is likely to notify the Compliance and Performance Support Officer who in the first instance should clarify with the data subject whether they wish for the OPCC to stop processing the personal information in its current state. If this is the case then the Compliance and Performance Support Officer must seek advice from the Data Protection Officer and notify the Chief of Staff and Monitoring Officer who will make a decision as to whether the restriction of processing is practical, reasonable and justified. If this is deemed to be the case, then the Compliance and Performance Support Officer will liaise with the information owners and restrict processing.

4.13.2 In order to ensure that OPCC data is accurate and up-to-date, the Compliance and Performance Support Officer must request from the data subject the correct information and where necessary, proof that the new information they are providing is accurate. The data subject is under no obligation to provide new information and it may be the case that the OPCC has to restrict processing and consider deleting the information.

4.14 Right to Erasure

4.14.1 The 'right to be forgotten' is inextricably linked to the restriction of processing, it may be the case that one follows the other. Where a data subject has received a response to their SAR and has identified that information about them is held by the OPCC, they may make an application to the OPCC for that data to be deleted.

4.14.2 Where a request is received, the Chief of Staff and Monitoring Officer must make the decision as to whether it is practical and justifiable to restrict the processing of personal information whilst a decision is made as to whether to erase that data. The Compliance and Performance Support Officer will liaise with information owners and ensure that processing is restricted for the duration determined by the Chief of Staff and Monitoring Officer. At all times, the Compliance and Performance Support Officer and the Chief of Staff and Monitoring Officer are to document their decisions and rationales so that the OPCC can provide information to the Information Commissioner's Office in a timely manner.

4.15 Retention

4.15.1 A copy of the completed response will be held by the OPCC for two years from the date the request is closed, in line with our retention schedule.

5. Training

5.1 The Compliance and Performance Manager and the Compliance and Performance Support Officer of the OPCC need to receive specific training in dealing with SARs.

6. Monitoring

6.1 Responsibility for monitoring this document will lie with the Compliance and Performance Manager. The document will be updated when changes to the guidance are made by the Information Commissioner's Office.

7. Consultation

7.1 This is a policy used by all Welsh OPCC's. The document was drafted by Gwent with each of the DPO's consulted in the other three OPCC's along with all four Chief Executives/Chief of Staff and Monitoring Officers.

8. Associated Documentation

8.1 The UK General Data Protection Regulation supersedes the previous EU directive and Act and give data subjects clearly defined rights and control over the personal data, with increased penalties for organisations for non-compliance. The Regulations cover the processing of all personal information whether it is processed on computer, CCTV, manual filing records, digitally or via any other form of media. The UK GDPR does not apply to the processing of personal data for specific law enforcement purposes.

8.2 The Data Protection Act compliments the UK GDPR. It details exemptions where the UK GDPR provisions do not apply, defines the powers of the Information Commissioner and clarifies some of the terms used in the UK GDPR. The Act also defines the circumstance and lawful basis under which the OPCC can process law enforcement data.

9. Dissemination

9.1 All staff working within the OPCC must be made aware of the SAR policy and procedure due to the nature of the roles undertaken. Any person is able to make a SAR at any time in any format and staff must be able to identify one and provide assistance on next steps. As such this policy will be circulated to all OPCC staff.

10. Review Period

10.1 The document will be reviewed every four years, on an all Wales basis, to ensure it remains accurate.

11. Appendices

11.1 Appendix A – Subject Access Request Form

All Wales Subject Access Form V2 May