OPCC Subject Access Policy

Document Approval and Identification

Author	Clare Rex
Version Number	1.2
Date	28/6/2022

Version History

Version No.	Version Issue Date	Authored / Revision by	Approved by	Reason
1.0	**1/11/2019**	**Clare Rex**	**Mike Richmond**	
1.1	**2/6/2020**	**Mike Richmond**	**Mike Richmond**	**Added working practice**
1.2	**28/6/2022**	**Mike Richmond**	**Mike Richmond**	**Added clarity around information sharing**
1.3	**25/6/24**	**Mike Richmond**	**Mike Richmond**	**Review, minor changes for clarity**

Contents

1. Introduction

1.1 The UK General Data Protection Regulations (UK-GDPR) place an emphasis on accountability for organisations regarding the way in which they handle personal data. The Office of the Police and Crime Commissioner for Humberside (OPCC) is committed to

protecting the rights of individuals with regard to the processing of their personal data and must be able to demonstrate compliance with the GDPR.

1.2 This policy clarifies the statutory rights that individuals have over their data and the procedures in place for ensuring that their rights are consistently met to ensure that we are able to respond to Subject Access Requests (SAR) and any related dissatisfaction in a timely, consistent manner and in compliance with the regulations.

2. Legislation

2.1 The UK-**GDPR** supersedes the previous EU directive and Act and give individuals 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 GDPR does not apply to the processing of personal data for specific law enforcement purposes.

2.2 The **Data Protection Act 2018** (DPA) complements the GDPR. It details exemptions where the GDPR provisions do not apply, defines the powers of the Information Commissioner and clarifies some of the terms used in the GDPR. The Act also defines the circumstance and lawful basis under which the OPCC can process law enforcement data.

3. Definitions

3.1 **Personal Data** is defined as information which relates to a living individual 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 an individual and any indication of the intentions of the data controller or any other person in respect of that individual.

3.2 **Processing** of personal data refers to the obtaining, recording, holding or performing any operation in any capacity, and applies to both manual and computerised records.

3.3 **Data Subject** refers to the individual to whom the personal information relates.

3.4 **Data Controller** is a person or an organisation who determines the purpose for which and manner in which personal data is to be processed.

3.5 **Data Processor** is any person or organisation who processes data on behalf of the Data Controller.

3.6 **Data Breach** is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, disclosure of or access to, personal data.

4. Data Subject Rights

4.1 GDPR provides for the following data subject rights to individuals regarding the processing of their personal data:

- The right to be informed how personal data is being processed
- The right of access to their personal data
- The right to rectification of inaccurate personal data (and to have incomplete personal data completed)
- The right to erasure
- The right to restrict processing of personal information
- The right to personal data portability
- The right to object where processing is carried out under public task or legitimate interest
- The right not to be subject to automated decision-making, including profiling
- The right to be informed of a data breach which poses a high risk to the rights and freedoms of individuals
- The right to complain to the Information Commissioner

4.2 Requests can be made in writing, via email or verbally and Data Subjects do not need to mention the legislation in exercise any of their rights

5. Right to be Informed

5.1 Data subjects have a right to be informed how their personal data will be processed by the OPCC.

5.2 The OPCC has published a comprehensive privacy policy detailing the required information necessary to be communicated to individuals when processing their personal data. This is

a regularly reviewed living document which can be accessed via the OPCC website here https://www.humberside-pcc.gov.uk/Privacy-Notice.aspx.

5.3 In the event of a Data Subject request regarding how their personal data will be processed they should in the first instance be directed to the OPCC privacy policy. If individuals do not have internet access when they must be provided with a paper copy or some other accessible format.

5.4 Should the Data Subject require any clarification or further information regarding how their data is used, refer the individual to the Data Protection Officer (DPO).

5.4 If asked, the data subject must be told of any recipients their data has been shared with.

6. Right to Rectification

6.1 Data Subjects have a right to have inaccurate information rectified, to have a supplementary statement of fact added and for any incomplete data to be completed.

6.2 The fourth Data Protection Principle requires that personal data shall be accurate and kept up to date and it is everybody's responsibility to ensure the accuracy of personal data on OPCC systems. Where rectification requests are straightforward such as misspelt names or an updated address then any member of the OPCC receiving such a request should action it promptly as necessary.

6.3 Should the Data Subject dispute the rectification of inaccurate data, the case should be referred to the SOM. The SOM will liaise with the Data Subject in order to obtain the necessary evidence to ascertain the facts in dispute.

6.4 Once evidence has been obtained by the SOM, the case will be referred to the Data Protection Officer (DPO) who will analyse the original information, its source and provenance and the evidence provided by the Data Subject. The DPO will make a decision as to the accuracy of the personal data based upon their findings.

6.5 Where the data is found to be inaccurate, it will be rectified or a supplementary statement added and the Data Subject will be informed by the DPO.

6.6 Where the data is proven to be accurate, the Data Subject will be informed by the DPO and also advised of their right of complaint to the Information Commissioner.

7 Data Subject Access

7.1 Any request for an individual's personal data in any format (written, verbal, email) should be logged on our secure database and referred to the SOM at the earliest opportunity, with confirmation of the date the request was initially received by the OPCC.

7.2 The SOM will undertake an assessment to ensure:

- There is sufficient evidence of the Data Subject's identity or whether additional proof of identity is required (such as passport, driving licence or recent utility bill). A proportionate approach will be taken to requesting additional proof of identification, taking into account factors such as longstanding relationships with a Data Subject (eg where a request is made from a historically known email account, address or telephone number) and the sensitivity of data requested.
- That the Subject Access Request is clear. If the request is in any way unclear, the SOM will contact the Data Subject to seek clarification. Where necessary, the SOM will liaise with the Data Subject about their interactions with the OPCC in order to ensure that all requested data can be located.

7.3 Third party requests for personal data will not be considered without written consent of the Data Subject and comprehensive proof of their identification. This includes partners, family members and friends.

7.4 The SOM will undertake a comprehensive search for relevant personal data across the suite of OPCC systems, with assistance from an appropriate Information Asset Owner (IAO) as required.

7.5 All personal information relating to individuals other than the data subject must be redacted from any disclosure in response to a SAR.

7.6 The SOM will provide a written response to the Data Subject within the statutory timeframe of one month from receipt of the request and a copy of the response will be saved within the secure database. The response will contain:

- Summary of searches undertaken in locating the personal data.
- If applicable, an explanation of whether and why the SAR has been refused.
- Clarification of the right to appeal to the Information Commissioner should the Data Subject have concerns in respect of GDPR compliance by the OPCC.

7.7 Any information sent by email must be password protected. Information sent by post must be double enveloped, signed for and marked Private and Confidential.

8 Complaints

8.1 A Data Subject who wishes to complain that the OPCC has breached GDPR, Data Protection or their privacy rights should be directed to the DPO at pcc@humberside.pnn.police.uk

8.2 Complaints which relate to a Data Breach will be dealt with in line with the OPCC Data Breach Policy.

8.3 All other complaints will be dealt with by the DPO who will assess what, if any, breach of GDPR has occurred and respond accordingly within 12 days of receipt of such a complaint. Any response must inform the Data Subject of their right to complain to the Information Commissioner.

Subject Access: Working Practice

Upon receipt of a SAR

- Verify whether you are controller of the data subject's personal data. If you are not a controller, but merely a processor, inform the data subject and refer them to the actual controller.
- Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.
- Verity the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not: request additional information.
- Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, you may refuse to act on the request or charge a reasonable fee.
- Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.
- Verify whether you process the data requested. If you do not process any data, inform the data subject accordingly. At all times make sure the internal SAR policy is followed and progress can be monitored.
- Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.
- Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

Responding to a SAR

- Respond to a SAR within one month after receipt of the request:

(i) If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month;

(ii) if the OPCC cannot provide the information requested, it should inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

- If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.
- If data on the data subject is processed, make sure to include as a minimum the following information in the SAR response:

(i) the purposes of the processing;

(ii) the categories of personal data concerned;

(iii) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules1 or EU model clauses;

(iv) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

(v) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(vi) the right to lodge a complaint with the Information Commissioners Office ("ICO");
(vii) if the data has not been collected from the data subject: the source of such data;
(viii) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

- Provide a copy of the personal data undergoing processing.

What must I do?

1. ***MUST***: On receipt of a subject access request you must **forward** it immediately to the Statutory Support Manager or, in their absence, the Data Protection Officer.

2. ***MUST***: We must correctly **identify** whether a request has been made under the Data Protection legislation

3. ***MUST***: A member of staff who receives a request to locate and supply personal data relating to a SAR must make a full exhaustive **search** of the records to which they have access.

4. ***MUST***: All the personal data that has been requested must be **provided** unless an exemption can be applied.

5. ***MUST***: We must **respond** within one calendar month after accepting the request as valid.

6. ***MUST***: Subject Access Requests must be undertaken **free of charge** to the requestor unless the legislation permits reasonable fees to be charged.

7. ***MUST***: Managers must ensure that the staff they manage are **aware** of and follow this guidance.

How must I do it?

- Notify the Statutory Support Manager or, in their absence, the Data Protection Officer] upon receipt of a request.
- You should clarify with the requestor what personal data they need.
    - They must supply their address and valid evidence to prove their identity.
    - They are not required to do so in writing but you may ask them to do so.

If additional proof of identity is required, the following forms of identification are accepted

(These documents must be dated in the past 12 months, +These documents must be dated in the past 3 months):*

- Current UK/EEA Passport
- UK Photocard Driving Licence (Full or Provisional)
- Firearms Licence / Shotgun Certificate
- State Benefits Entitlement Document*
- State Pension Entitlement Document*
- HMRC Tax Credit Document*
- Local Authority Benefit Document*

  - HMRC Tax Notification Document
  - Disabled Driver's Pass
  - Financial Statement issued by bank, building society or credit card company+
  - Judiciary Document such as a Notice of Hearing, Summons or Court Order
  - Utility bill for supply of gas, electric, water or telephone landline+
  - Most recent Mortgage Statement
  - Most recent council Tax Bill/Demand or Statement
  - Tenancy Agreement
  - Building Society Passbook which shows a transaction in the last 3 months and your address
- Depending on the degree to which personal data is organised and structured, you will need to search:
  - emails (including archived emails and those that have been deleted but are still recoverable),
  - Word documents,
  - spreadsheets,
  - databases,
  - systems,
  - removable media (for example, memory sticks, floppy disks, CDs),
  - tape recordings,
  - paper records in relevant filing systems etc. which your area is responsible for or owns.
- You must not withhold personal data because you believe it will be misunderstood; instead, you should provide an explanation with the personal data. You must provide the personal data in an "intelligible form", which includes giving an explanation of any codes, acronyms and complex terms. The personal data must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort. You may be able to agree with the requester that they will view the personal data on screen or inspect files on our premises. You must redact any exempt personal data from the released documents and explain why that personal data is being withheld.
- A spreadsheet is maintained allowing the OPCC to report on the volume of requests and compliance against the statutory timescale.
- When responding to a SAR, we must advise the requestor that they may complain to the Information Commissioners Office ("ICO") if they remain unhappy with the outcome.

Sample letters

All letters must include the following information:

a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules3 or EU model clauses
d) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with the Information Commissioners Office ("ICO");
g) if the data has not been collected from the data subject: the source of such data;
h) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Replying to a subject access request providing the requested personal data

[Name]
[Address]
[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your [letter/email] of [date] making a data subject access request for [subject]. We are pleased to enclose the personal data you requested.

Include (a) to (h) above.

Yours sincerely

Release of part of the personal data, when the remainder is covered by an exemption

[Name]
[Address]
[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your [letter/email] of [date] making a data subject access request for [subject]. To answer your request we asked the following areas to search their records for personal data relating to you:

• *[List the areas]*

I am pleased to enclose [some/most] of the personal data you requested.

[If any personal data has been removed] We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you. You will notice that [if there are gaps in the document] parts of the document(s) have been blacked out.

[OR if there are fewer documents enclose] I have not enclosed all of the personal data you requested. This is because [explain why it is exempt].

Include (a) to (h) above.

Yours sincerely

Replying to a subject access request explaining why you cannot provide any of the requested personal data

[Name]
[Address]
[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your [letter/email] of [date] making a data subject access request for [subject]. I regret that we cannot provide the personal data you requested. This is because [explanation where appropriate].

[Examples include where one of the exemptions under the data protection legislation applies. For example the personal data might include personal data is 'legally privileged' because it is contained within legal advice provided to the OPCC or relevant to on-going or preparation for litigation. Other exemptions include where the personal data identifies another living individual or relates to negotiations with the data subject.

Yours sincerely