Subject Access Request Procedure

Upon receipt of a SAR

- Verify whether you are the correct data controller of the personal information that the data subject has requested.
    - If you are not a controller, but merely a processor, inform the data subject and refer them to the actual controller.
    - The request may also be for information held by the local police force – if this is the case you need to reply to inform them of this and how they can make this request to the force.
- Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.
- Verify 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, inform the data subject of any costs involved in the processing of the SAR and provide a date by which a response should be expected.
    - If a request for clarity is made to the data subject then the timeframe in which a response must be provided is paused. This must be communicated to the data subject when requesting clarity.
    - If a request for further evidence as to the ident of the data subject is made, then the timeframe in which a response must be provided is paused. This must be communicated to the data subject when requesting clarity.
- 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 individuals and make sure this data is filtered before the requested data is supplied; if data cannot be filtered, ensure that other individuals 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:
    - 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;
    - 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 information on the data subject is processed, make sure to include as a minimum the following information in the SAR response:
    i. the purpose for the processing of their data;
    ii. the categories of personal data concerned;
    iii. the recipients or categories of recipient you disclose the personal data to;
    iv. your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
    v. the existence of their right to request rectification, erasure or restriction or to object to such processing;
    vi. the right to lodge a complaint with the Information Commissioner;
    vii. information about the source of the data, where it was not obtained directly from the data subject;
    viii. the existence of automated decision-making (including profiling); and
    ix. the safeguards you provide if you transfer personal data to a third country or international organisation.

- A lot of the above is likely to be included in a privacy notice – where this is the case a link to the privacy notice

- 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 Governance Officer, 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 (both electronic and hard copy).

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 Governance Officer 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, 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 data subject 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 data subject that they may initial make a complaint to the OPCC if they are unhappy with the outcome and if still not satisfied can complain to the Information Commissioners Office (ICO).