



Subject Access Request (SAR) Procedure

Data Protection Act 2018

Information Assurance Group

January 2020

Version 1.1

Document Control Sheet

Name of Document:	Subject Access Request (SAR) Procedure
Author	Alison Morris, Records and Heritage Manager (R&HM)
Consultees	Information Assurance Group: including: Mike Alexander, ICT Security Officer Sheila Campbell, Principal Librarian Sean Hoath, Senior Solicitor Kathryn McPherson, Senior Solicitor Atholl Scott, Internal Audit Manager Roddy Huggan, Commissioning Manager FOI Team: Sophie Ward, Information Coordinator, Scott Reid, Local Heritage Officer (and FOI cover)
Description of Content	Guidance for staff on how the Council processes a Subject Access Request (SAR)
Distribution:	Council wide upon approval
Status	Version 1.1
Date	Nov 2018 Apr 2019 January 2020

Contents

Definitions	4
1.0 Introduction.....	5
1.1 Information Commissioner’s Office (ICO).....	5
1.2 FOI Team	5
2.0 Handling a SAR – the Process	5
2.1 Identifying and/or receiving a SAR	5
2.2 Logging a request	6
2.3 Collating info	6
2.4 Redaction	6
2.5 Copies.....	7
2.6 Collection	7
2.7 Closure.....	8
3.0 Who can make a SAR?	8
3.1 Requests on behalf of another data subject.....	8
Children	8
Parental Rights	8

Agents	9
3.2 Further permissions	9
3.3 Deceased Individuals	9
4.0 Timescales	9
4.1 Fulfilling a request.....	9
4.2 Extensions.....	9
4.3 Lack of communication	10
5.0 Formats	10
6.0 Routine versus Deliberate Deletion of Information	11
7.0 Advice and Support	11
8.0 Exemptions.....	11
8.1 Third Party Information.....	11
8.2 Legal Advice.....	12
8.3 Harm – Health, Social Work and Education	12
8.4 External organisations.....	12
8.5 Crime and Taxation	12
8.6 Confidential references	12
8.7 Negotiations with the Requestor	12
8.8 Requests for non-personal information	12
9.0 Charging.....	13
9.1 Manifestly unfounded or excessive requests.....	13
9.2 Further copies	13
9.3 Factually incorrect information	13
9.4 Retention of SARs and the first redacted copies.....	13
10.0 Stats.....	13
11.0 References and Links	13
12.0 Contacts.....	14

Definitions

Data controller: A body that determines the purposes for and manner in which personal data is used. This includes employees of the data controller. The Council is considered to be the data controller for most of its activities that involve personal data.

Data subject: A living individual to whom personal data relates.

Personal data: Any information relating to a data subject, particularly information that can be used to identify them such as: a name, an identification number, location data, an online identifier; or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual – e.g., a manager's assessment of an employee's performance during their probation period.

Special Category Data (also referred to as **Sensitive Personal Data**): This is personal data consisting of information as to any of the following:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetics.
- Biometrics (where used for ID purposes).
- Health.
- Sex life.
- Sexual orientation.

Special category personal data is subject to much stricter conditions of processing. Personal data relating to criminal convictions and offences are not included but similar extra safeguards apply to its processing.

1.0 Introduction

The Data Protection Act 2018 (DPA 2018) and the EU General Data Protection Regulation (GDPR) gives individuals the right to access personal information about themselves held by an organisation. Article 15 of GDPR sets out this right and such a request is known as a Subject Access Request (SAR). Compliance with such a request is therefore a statutory duty. The FOI team coordinates these requests; collating information, overseeing redaction and managing their collection.

Guidance on Data Protection, the Council's Data Protection Policy and other Information Rights are available on the [Information Management > Data Protection interchange page](#).

Information on how to exercise Rights under Data Protection is available on the Council's [Data Protection internet pages](#); including a specific guide on [Your Personal Data Rights](#) and a [SAR form](#) (with corresponding Privacy Notice) are available.

1.1 Information Commissioner's Office (ICO)

The Data Protection Act is regulated and enforced by the Information Commissioner's Office (ICO). Their website has examples and guides on how to comply with Data Protection legislation; ico.org.uk. The ICO can be applied to if a requestor is dissatisfied with our handling of a SAR. It is imperative that all SARs are dealt with correctly and promptly.

1.2 FOI Team

Access to Information requests are handled by the FOI Team. Requests predominantly include Freedom of Information Requests (FOIs), Environmental Information Regulation Requests (EIRs) and Subject Access Requests (SARs). Other requests are usually handled by departments, such as Pupil's Education Records requests are handled by the relevant school.

The FOI Team consists of the Records and Heritage Manager and the Information Coordinator.

2.0 Handling a SAR – the Process

2.1 Identifying and/or receiving a SAR

Any request made verbally or in writing must be handled via this procedure, regardless of whether the data subject has completed a specific form or not. Indeed a request is valid even if the request does not use the term 'subject access request' or reference Data Protection legislation. All SARs should be passed promptly to the FOI Team (info@moray.gov.uk).

Some SARs are mistakenly submitted as Freedom of Information (FOI) requests; these are picked up by the FOI team. Similarly, if a SAR does not concern personal information then their request would actually need to be processed as a FOI, although it is usually appropriate to clarify this with the requestor first.

If a verbal request is made then the data subject can be directed to the online information, SAR form and/or prompted to make the request in writing to the FOI team. However, a verbal request should not be discounted if they do not reconfirm their request in writing.

In order to answer a request as efficiently as possible any clarification on the scope of a request should be done at the earliest opportunity, if that is before the actual request is received this can be managed by departmental staff, if it is after the request is received then it can be done by the FOI Team.

The appropriate Privacy Notice is already attached to the SAR Form.

2.2 Logging a request

Requests are logged by the Information Coordinator onto Lagan, details for this are in the FOI Team Guide. If anything is unclear or missing then clarification will be sought from the requestor; the clock will be paused whilst clarification/verification is sought (see below for more on set timescales). The FOI team will be the single point of contact for the requestor so all clarification requests are handled by the FOI Team.

2.3 Collating info

The Information Coordinator will contact relevant department(s), ask for the information requested, and, stipulate a short deadline. The requestor has a right to personal information whether it is held electronically or in hardcopy (paperwork).

Departments will need to provide copies of the information they hold; normally this should be photocopied or printed single sided and without staples. If there are any issues with providing copies please contact the Information Coordinator. Paperwork can either be transferred via internal mail or dropped off by a member of staff, again please liaise with the Information Coordinator.

When there is a small amount of information then departments are welcome to liaise with the Information Coordinator to organise providing electronic copies.

2.4 Redaction

Only information that identifies and relates to the data subject may be given. Therefore it is important that the information is checked and all other personal details are removed.

Staff names, work contact details and professional/work opinions are not redacted but personal details are redacted, such as staff having sick days, holidays or similar personal information (including clearly stated personal opinions). Signatures are also removed. There are also a few other exemptions for information, see below for further details. The FOI Team will provide advice and guidance throughout the redaction process.

Redaction is undertaken by at least one member of staff from the originating department who, where possible, is familiar with the data subject/type of information

with assistance and support from the Records and Heritage Manager and Information Coordinator. If there are any particular details that need to be considered, such as parental rights or if a court order forbids the data subject knowing some details, then these should be highlighted by the Department before redaction is started.

Please be aware that departmental staff must be made available to undertake redaction, which can be time consuming, however, it cannot be avoided. The amount of time that redaction takes is monitored as it can take numerous afternoons to complete; the adage 'many hands make light work' is certainly apt.

Redaction is undertaken in Elgin Library, either in the R&HM's office or in the small meeting room. This avoids having to transport potentially large quantities of personal information outside the office.

Small quantities of information can be electronically redacted using Adobe Pro, for which the Information Coordinator has a license. Most redaction is undertaken manually on paper with permanent markers.

2.5 Copies

The redacted copy is then photocopied by the Information Coordinator; it is this photocopied redacted version that is made available to the requestor. Copies are produced on a darker setting to ensure that redaction is absolute.

Once copying and redaction is complete the originals are returned to the department(s).

Any pages that are withheld, for example duplicates or information that is in the relevant file but does not identify or relate to the data subject, are stored with the redacted copy. The redacted copy is kept for reference; once the SAR is closed this copy is sent to the Closed Records Store; the Information Coordinator organises this.

2.6 Collection

The FOI Team contact the requestor and inform them that the copies are ready to collect.

If the requestor is collecting in person then identification is checked by the FOI Team and the date and time of collection are noted. If it is to be collected by another person on their behalf, such as a solicitor or advocate, then prior notification of this as well as identification checks and association checks are made, again date and time of collection are logged.

If the requestor is being sent the information electronically then the Information Coordinator does this using emails that are encrypted and password protected (see FOI Team Guide).

If the requestor requires the paperwork to be sent, couriers are used and usually sent to another institution that can verify the identity of the requestor, e.g. another local authority, a police station, solicitor's office etc. (see FOI Team Guide for details). For information on charges, see section 9 of this guide.

The FOI Team will also ensure that information is given to the requestor about redacted information, details on how to contact us if there are any problems with the information provided, and, contact details of the ICO if they are dissatisfied.

2.7 Closure

Once the SAR is fulfilled then the request can be closed (on Lagan – see FOI Team Guide). Other tasks the FOI team will ensure are completed include; returning original files to the department(s), sending the redacted copy to the CRS, and, logging the number of hours and other details.

3.0 Who can make a SAR?

All data subjects have a Right of Access and can submit a SAR.

3.1 Requests on behalf of another data subject

Usually an individual can only request information about themselves, but there are occasions when a request may be made on behalf of another data subject. For the request to be valid the requestor must prove they have a right of access to that data subject's information, such as Power of Attorney.

Children

When information is about a child that child is still the data subject and that information belongs to that child, however, there are slight variations on access.

In Scotland a child that is 12 years or over and presumed to be of sufficient maturity and understanding may submit their own SAR; they do not require the permission of a parent or other adult with parental rights and responsibilities for them.

If the child is under 12 or deemed to have insufficient understanding then an adult with the rights and responsibilities for the child can make the request on the child's behalf.

If a child under 12 years requests direct access to their own information then this will be assessed on a case by case basis and be influenced by their understanding of their Rights and, where applicable, in consultation with Social Work.

Parental Rights

For children under 12, when a requestor has parental rights and responsibilities they are allowed access to the child's information.

However, if the child is over 12, or deemed capable of fully understanding the request, then the child's permission must be sought.

Agents

Solicitors and MPs/MSP

A solicitor who says they act for a person stands in their shoes and has the authority to make the same request as the person. Similarly an MP or MSP have special exemptions when seeking information on behalf of constituents. However, given the potential consequences for data breaches and the often extremely sensitive information involved it is our practice to request a mandate. This practice is in line with other Council practices, such as Complaints.

Advocates

If an advocate is acting on behalf of a data subject then a signed mandate or similar confirmation of the data subject's wishes for this representation is required. When a data subject has utilised the resources of representation but has not provided a signed mandate then no personal information can be passed to that representative, however, information explaining this and explaining how a SAR can still be completed should be provided.

3.2 Further permissions

Information that identifies and relates to the data subject may be contained within information relating to other data subjects; where feasible it is practical to request permission for the other data subjects for their information to also be released. For example, in a Social Work file there would likely be information about immediate relatives such as siblings, parents and/or spouses, seeking their permission would save significant redaction time.

3.3 Deceased Individuals

Data Protection legislation only applies to living individuals, although there are exemptions such as for health data. Nonetheless it is best practise to only release information to a confirmed personal representative.

Freedom of Information requests can be made for information that is not personal; some deceased information may therefore be accessed in this way.

4.0 Timescales

4.1 Fulfilling a request

Once a request is received we have **1 calendar month** to complete it. As such it is important to identify an SAR as quickly as possible and promptly pass it to the FOI Team. The FOI Team will monitor the deadline.

4.2 Extensions

An extension may be applied to certain requests:

- If further information is required to complete the initial request then we can pause the clock whilst this information is being provided; e.g. clarification of identify or verifying rights and responsibilities.
- The request is deemed to be complex (potential 2 month extension and/or charge of a reasonable fee to account for the administrative cost of processing the information)
- The requests are deemed to be numerous (potential 2 month extension and/or charge of a reasonable fee)

Data subjects should be informed of any extension or delay and the relevant reasons for them.

4.3 Lack of communication

If further clarification is required this is requested by the Information Coordinator, however, if no reply is received then the requestor is contacted again after 1 month. This follow up contact will ask the requestor to communicate with the Information Coordinator to acknowledge they still require the SAR, it will reiterate the details still required for the SAR to proceed and specify a deadline for reply (the deadline is usually 2-4 weeks but will vary according to end of quarter dates). The follow up contact will also include notice that if no response is received within the deadline that the request will be closed, as well as contain details on how to resubmit a SAR at a later date. If after this deadline no further contact has been received then the SAR will be closed.

5.0 Formats

All information held that identifies and relates to the data subject may be required to complete a SAR regardless of medium; all paper and electronic records are covered, including emails, database details and handwritten notes.

Information should be provided in a concise, transparent, intelligible and accessible form. As such if information is held in a format that requires codes or a key to understand it then those codes or key should also be provided. Where handwritten notes are provided, even if the handwriting is difficult to read, a transcript is not required.

Ideally completed requests should be communicated to the requestor in the same medium by which the request was received. Furthermore, the legislation states that where possible the data controller should be able to provide remote access to a secure system that would provide a data subject with direct access to their personal data¹; this should certainly be considered when new systems and online resources are developed.

¹ Recital 63 and article 15 GDPR

6.0 Routine versus Deliberate Deletion of Information

SARs relate to information held at the time the request is made. If information becomes available or is amended during the processing and fulfilment of the request then that information should also be considered. However, it is not acceptable to amend or delete information if this would not have been routinely done so before the request, for example electronic backups and recycle bins that are routinely purged are fine, but if information was deliberately deleted to prevent disclosure then this would be an offence under the DPA 2018.

7.0 Advice and Support

There can be occasions whereby it is not in the best interests of the data subject to be provided with all the information they have requested, for example if someone has requested a Social Work file it may be better for the data subject to spend some time going through the actual file with a Social Worker. This method allows for explanations regarding why certain forms were produced or certain processes followed that will enable the data subject to understand their file and personal information better.

These are exceptions and if such support is not accepted the request should still be completed.

8.0 Exemptions

There are a few exemptions available to allow refusal to provide some information as part of a SAR.

It is good practice to clearly mark information with any relevant exemption to assist with possible future disclosure, for example some medical letters have confidentiality clauses stating that the letter cannot be reproduced without express permission of the author/authorising organisation.

8.1 Third Party Information

As previously highlighted only information that identifies and relates to the individual has to be provided, similarly if personal information identifies and relates to any third parties then it must be withheld, unless we have their express permission to release it. If a request is repeated then these permissions need to be renewed as well.

Professional opinions and names are retained, however, any personal information about staff, such as comments regarding absences, counts as third party information and should be removed.

8.2 Legal Advice

Legal Advice communicated between legal professionals and their clients is exempt due to legal professional privilege². This does not apply to other professionals.

8.3 Harm – Health, Social Work and Education

If including certain personal information about the data subject's health or Social Work record could negatively impact on the data subject's physical or mental health, then disclosure should be considered carefully in consultation with the appropriate professional and consideration of the stringent serious harm test³. Hopefully the appropriate professional will be involved in the redaction process as exemption and redaction may be appropriate.

8.4 External organisations

Copies of material provided from external bodies that were not commissioned by Moray Council and are not our intellectual property should not be released. However, we can inform the requestor that these copies are held and how to contact the appropriate organisation to request their personal information, for example Social Work files may hold copies of letters or reports from the NHS.

8.5 Crime and Taxation

Information can be exempt if its disclosure would prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, or the collection of any tax or duty. For example if an individual is currently being investigated for council tax fraud then disclosing all information we hold on that individual could impact on the investigation.

8.6 Confidential references

Confidential references either provided or received by the Council about the data subject are exempt from disclosure.

8.7 Negotiations with the Requestor

Information about the Council's intentions in negotiations with an individual may be exempt as this could prejudice the negotiations. For example, information relating to employee tribunal proceedings. See Section 45 (4)(a).

8.8 Requests for non-personal information

SARs relate to personal data, if a request is made of general or non-personal information then this should be treated as a Freedom of Information Request (FOISA). The FOI Team will inform requestors if their request will be processed under different Access to Information legislation.

² DPA Schedule 2, Part 4, 19

³ [DPA 2018 Schedule 3](#)

9.0 Charging

There is no fee for SARs.

9.1 Manifestly unfounded or excessive requests⁴

However, if the request is found to be manifestly unfounded or excessive, or if it is repetitive, then the Council may:

- charge a reasonable fee to account for the administrative cost of processing the information; or
- choose not to fulfil the request. The data subject should be informed of the reasons the Council is not taking action, and they will have the right to make a complaint to the ICO and/or appeal to the courts for this right to be enforced.

9.2 Further copies

If an individual requests further copies of their data following a request then 'a reasonable fee' based on the administrative costs of providing further copies may be charged.

9.3 Factually incorrect information

Correcting factually incorrect information is not part of the SAR process and should be handled separately by departments. For example, if during the redaction process data about a different data subject unconnected with the file is found and has clearly been misfiled, this will be highlighted to the originating department to deal with the misfiled elements at their discretion.

9.4 Retention of SARs and the first redacted copies.

The first redacted copies are transferred to the Closed Records Store. They are retained for 3 years after the request has been completed, then securely destroyed.

10.0 Stats

The Information Coordinator collates SAR statistics on a quarterly basis. The number of SARs and whether they have been completed within their deadlines is reported within the Council and to the Scottish Information Commissioner.

These can be found here: <https://stats.itpublicknowledge.info/>

The Information Coordinator also records the number of hours taken to complete each SAR.

11.0 References and Links

Data Protection Act 2018 (DPA 2018)

<http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

⁴ [DPA 2018 12 Part 3, Chap 3, Supp, Sec 53](#)

General Data Protection Act (GDPR)

<http://www.privacy-regulation.eu/en/index.htm>

Scottish Information Commissioner:

<http://www.itspubliknowledge.info/>

The Information Commissioner's Office:

<https://ico.org.uk/>

Moray Council's Website pages:

Information Management

http://www.moray.gov.uk/moray_standard/page_41220.html

Freedom of Information

http://www.moray.gov.uk/moray_standard/page_53728.html

Data Protection

http://www.moray.gov.uk/moray_standard/page_41179.html

All Council fees

http://www.moray.gov.uk/moray_standard/page_54971.html

Moray Council's Intranet Pages:

Information Security (inc. FOI, DPA)

http://intranet.moray.gov.uk/Information_management/information_security.htm

Records Management (inc. Retention Schedules, Confidential waste etc.)

http://intranet.moray.gov.uk/Information_management/records_management.htm

12.0 Contacts

FOI Team:

Information Co-ordinator

Elgin Library

info@moray.gov.uk

Tel 01343 562644

(Please note this is not a full time post and working hours are currently Monday to Friday 12noon to 5pm.)

Records and Heritage Manager

Elgin Library

records@moray.gov.uk

Tel 01343 562633