Nottinghamshire County Council

Subject Access Request Procedure

At a glance

1. This document sets out Nottinghamshire County Council's approach to fulfilling its obligations in respect of the right of access, commonly referred to as a subject access request or 'SAR' which gives individuals the right to request a copy of any of their personal data held by an organisation.
2. It forms part of the suite of documents that comprise the Council's Information Governance Framework and sits under the Information Rights Policy.
3. It will be of particular relevance to those parts of the Council which actively deal with SARs requests, namely the Complaints and Information Team and HR but also other services who may deal with more specific requests for personal information.
4. Subject access requests can be made verbally or in writing and all staff must recognise and know how to deal with such requests.
5. The Council must respond to subject access requests within one month, or three months for complex requests.
6. The Council is not able to disclose information that would contravene someone else's rights under the UK GDPR or Data Protection Act.
7. Some information may be exempt from disclosure, and the Council can refuse to comply with a manifestly unfounded or excessive request
8. Staff should always remain mindful of information you create especially in emails you send, as these may have to be disclosed under legislation.
9. It is a criminal offence to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information a person making a SAR would have been entitled to receive

Background

10. The Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR) gives individuals the right to request a copy of any of their personal data as well as other supplementary personal information for example, photographs, audio messages and CCTV images.

11. The right of access gives individuals (referred to as data subjects in the context of data protection) the right to request access to their personal information which is being processed by a data controller. A data controller is an organisation or person which determines how and why personal data it uses, is processed. Nottinghamshire County Council is a data controller for the personal data it processes.

12. The Information Commissioner's Office (ICO) is independent regulator of data protection and freedom of information legislation in the UK and was set up to uphold information rights.

Definitions

13. "**We**" means the County Council and includes all members, employees, trainees / apprentices and volunteers of the County Council and contractors, suppliers and partners delivering County Council services on our behalf.

14. **Information** is used here as a collective term to cover terms such as data, documents, records and content, audio recordings, digital and photographic images etc. and can be on paper or electronic.

15. **Processing** is any operation or set of operations which is performed on personal information such as collection, recording, storing, alteration, combining, retrieval, use, disclosure, destruction etc.

16. **Personal data** in the context of SARs means any identifiable data or information relating to a living individua. This can be held in any format and (e.g., paper; electronic photographs; audio / visual recordings; CCTV images; microfiche etc)

17. A **data subject** is the person whose personal data is being processed.

Scope

18. This procedure does not cover:

    a) **Use of redaction software**. There is guidance on why and what to redact when disclosing personal or other confidential data to third parties Redaction and disclosure guidance. It is anticipated that further guidance will be issued on the use of redaction software, following completion of a piece of work to establish which software the Council will use for redaction going forward.

    b) **Deceased persons' records** which are covered by a separate procedure Information about the deceased

Who can make a SAR and how do they make it?

19. Subject access requests can be made by:

    a) The individual data subject themselves. This includes children as there are not any age requirements attached to the right of access, but it is common practice to consider 12 as the age where young people can exercise their own legal rights.

    b) Individuals requesting access on behalf of a child for whom they have parental responsibility

    c) A representative nominated by the individual to act their behalf such as solicitors or a relative, where there is valid consent by the individual granting the authority

d) In certain situations, a person granted an attorney or agent by the Court of Protection on behalf of an adult who is incapable of consent

20. Under ICO guidance, an individual can make a SAR verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact. It is also worth noting that individuals aren't required to use the technical term for a request ('SAR' or 'subject access request').

21. It is important that all employees know how to recognise a SAR and how to respond to it. This will be referenced in relevant intranet guidance (see Subject Access Requests and in mandatory information governance (IG) training for staff.

22. There are online forms to enable people to make a SAR on the Council's website: Request Personal Information – Subject Access Request.

23. The Council need to be satisfied about the identity of the requester, to ensure that personal data is only disclosed to those with a right to see it. Individuals will be required to provide two forms of identification before a SAR is processed - photo ID to confirm identity and another which confirms the requester's current address.

24. Where an application is made on behalf of an individual, consent must accompany the written application. The application must clearly identify the person in question, and the records required. Whilst individuals can request all of the information the Council holds about them without clarification, they are usually receptive to being more specific when prompted as this enables their request to be dealt with more quickly.

25. Postal, electronic and verbal requests will be routed to accessto.records@nottscc.gov.uk and will be coordinated by the Complaints and Information Team.

What information can be requested as part of a SAR?

26. Individuals have the right to obtain a copy of their personal data, as well as other supplementary information. It helps individuals to understand how and why the Council is using their data, and check it is doing it lawfully.

27. If a request seeks only information about a specific incident, or routine information, it may be gained by asking for it directly from the department holding it, without having to go through the Subject Access Request procedure. If this is not possible, the request will be processed as a Subject Access Request.

How long has the Council got to respond to a SAR?

28. The Council is required to respond to non-complex SARs promptly within **one calendar month** from receipt of the request and valid proof of identity. The time limit is calculated from the day the request is received, (whether it is a working day or not) until the corresponding calendar date in the next month.

29. If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

30. If the corresponding date falls on a weekend or a public holiday, we have until the next working day to respond.

31. This means that the exact number of days we have to comply with a request varies, depending on the month in which an individual makes the request.

32. For practical purposes, if a consistent number of days is required (e.g., for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

33. In **complex cases** the timescale for response can be **extended by a further two months**.

34. If a request is deemed to be complex, the Council must inform the requestor as soon as possible and within a month of the request being submitted. This communication will explain why the request is deemed complex and give a revised deadline for the response. Failure to do this is breach of the DPA 2018 and could lead to a complaint to the ICO.

35. The more general a request is, the more likely it is that there will be a delay or even a refusal of the request. Delay may occur if a request covers a high volume of data or if we require additional information from the requester before we are able deal with the request. To avoid delay or refusal, requests should be clear about the information sought and, where applicable, the time period the search is to cover.

What information needs to be provided in response to a SAR?

36. The scope of the information searches carried out are dependent on what information has been requested. For example, an individual may ask to see all their social care records between certain dates. Social Care SAR searches are generally carried out on the following systems:

    - Mosaic (Social Care Case Management System)
    - Wisdom (Records Management System) for the Council's stored, inactive paper records.
    - Solutions 4 Data SharePoint Online Records Repository – the Councils stored, inactive records / old microfilm records.

37. Email searches will only be carried out where records are currently in live email accounts (i.e., in the inbox or deleted box). Ordinarily there will be no requirement to retrieve information from any back-ups that may exist.

38. The right of access does not entitle the requestor to receive full copies of original documents held by the Council – only the personal information contained in the document. This means that on certain occasions the Council may choose to provide personal information as a chronology or summary, rather than the original documents.

How is the complexity of SARs decided?

39. Whether a request is complex depends upon the specific circumstances of each case. The size and resources of an organisation are likely to be relevant factors. As a large organisation with dedicated resources, the Council will ordinarily need to be clear about the reasons when determining a SAR to be complex.

40. The following are examples of factors that may, in some circumstances, add to the complexity of a request. The Council will need to demonstrate why the request is complex in the particular circumstances.

    - Technical difficulties in retrieving the information – for example if data is electronically archived.
    - Applying an exemption that involves large volumes of particularly sensitive information.
    - Clarifying potential issues around disclosing information about a child to a legal guardian.
    - Any specialist work involved in obtaining the information or communicating it in an intelligible form.
    - Needing to obtain specialist legal advice. If you routinely obtain legal advice, it is unlikely to be complex.
    - Searching large volumes of unstructured manual records (only applicable to public authorities).

41. Requests that involve a large volume of information may add to the complexity of a request. However, a request is not complex solely because the individual requests a large amount of information.

42. Also, a request is not complex just because we have to rely on a data processor (an organisation that processes data on behalf of the Council) to provide the information we need in order to respond.

Can we charge a fee for responding to a SAR?

43. Nottinghamshire County Council has never charged a fee for complying with a SAR, even when it was possible under the Data Protection Act 1998.

44. It is possible to refuse to comply with a manifestly unfounded or excessive request. For information about when a request may be manifestly unfounded or excessive, please see the ICO guidance 'When can we refuse to comply with a request?'.

Who in the Council is responsible for responding to a SAR?

45. Responsibilities for dealing with SARs within the Council are as follows:

Type of request	**Dealt with by**
Requests by current or former employees (e.g., requests for personal information pertaining to	HR

disciplinary proceedings)	
All other requests (e.g., requests for entire social care case records etc)	Complaints & Information Team
Routine, straightforward requests, typically for specific information (e.g., a person requestion a copy of their Care and Support Plan). Note these are typically not corporately recorded as SARs but the requirement to respond is on the terms set out in this document, as a minimum.	The relevant service area

46. Each service area with responsibility for undertaking SARs will have a detailed business process setting how SARs will be responded to. This will as a minimum include how and by who SARs are logged; reported on; in scope personal information is gathered; in scope personal information is redacted, checked and prepared; securely dispatched; retained, ultimately destroyed.

47. The SARs process for the Complaints and Information Team is linked at the end of this document. All requests dealt with by the Complaints and Information Team will be entered into Infreemation (the SAR case management system) and this will be maintained to monitor compliance to ensure all requests are answered in in accordance with legislative requirements.

48. The SARs process for HR is linked at the end of this document. HR will use their own system for logging and managing SARs but will ensure that their performance data is shared with the Complaints and Information Team so that a composite view of the Council's SARs performance can be established and regularly reported to the Information Governance and Cyber Security Board.

49. For other parts of the business, records should be kept on the appropriate case management system where a request for personal information has been made and responded to.

Can a Subject Access Request be refused or information withheld?

50. The Council is obligated to always try to give a person the data they have asked for in a SAR. However, sometimes it might be appropriate to withhold some or all of the information that someone has asked us to provide. This will typically be where an exemption to the right of access applies as detailed in detailed in Schedules 2-4 of the DPA 2018.

51. Exemptions must not routinely be relied upon or applied in a blanket fashion. They must be considered on a case-by-case basis.

52. In line with the Council's accountability obligation to evidence how it complies with data protection legislation, reasons for relying on an exemption must always be documented.

53. Where an exemption does not apply, we must comply with the SAR request.

54. The most used exemptions for the Councils records are:

Health Data: DPA 2018, Schedule 3, Part 2	Exempts disclosure to a data subject where the data relates to health data.
Serious Harm; DPA 2018, Schedule 3,	The serious harm test is met if disclosing the data would be likely to cause serious harm to the physical or mental health of the data subject or another individual.
Legally Privileged Information: DPA 2018, Schedule 2, Part 4	Personal information covered by legal professional privilege
Social Work data: DPA 2018, Schedule 3, Part 3	Restricts the rights of access by a data subject where the data relates to social work data.
Child abuse data: DPA 2018, Schedule 3, part 5, para 21	Exempts the disclosure of personal data where the data subject is or has been the subject of or may be at risk of child abuse to the extent it would not be in the best interest of the data subjects.
Protection of the Rights of others: DPA 2018, Schedule 2, Part 3.	Provides an exemption that can apply if where a SAR covers information containing the personal data of more than one individual. See next section)

55. The full list of exemptions can be found at the following link Exemptions | ICO.

What if the request involves information about other individuals?

56. Individuals are only entitled to access their own personal data under a SAR. However, personal data can relate to more than one person. Therefore, responding to a SAR may involve providing information that relates to both the requester and another individual.

57. For instance, an employee's personnel file is likely to contain information identifying managers and colleagues who have contributed to (or are discussed in) that file. This requires that we reconcile the requesting employee's right of access with the third parties' rights in respect of their own personal data.

58. Detailed guidance on judging whether to apply the exemption that relates protection of the Rights of others (DPA 2018, Schedule 2, Part 3) can be found at the following link What should we do if the request involves information about other individuals? | ICO. At high level this poses the following key questions:

    a) Does the request require disclosing information that identifies another individual?
    b) Has the other individual provided consent?
    c) Is it reasonable to disclose without consent?

59. In line with the application of all exemptions, a record must be kept of the rationale for the decision to withhold or disclose information about others.

What checks should take place on the SAR response prior to release?

60. The completed SAR should be peer checked by scanning through the document(s) to see if redactions have been fully applied and the documents are

readable. This may involve selecting a random sample of pages throughout the document for checking.

61. A **watermark will be applied** to all documents which are to be released to the requestor. Wording to be used may be “Data Subject Copy” or “Requestor Copy”. The watermark should have some transparency where it covers the data on the page and should be visible when printing and visible on-screen. The setting should be 20% opacity and an angle of 45 degrees.

62. Each document must then be **encrypted and secured against editing**, so the watermark cannot be removed by the requestor.

63. A copy of the copies of the original unredacted documents, the **final redacted documents**, **summary of redactions** and **explanation of redactions** should be saved within the appropriate business repository for SARs.

How should SAR information be sent to a requestor?

64. The SAR response must be accompanied by a cover letter and there are specific items within the letter which ICO guidance says should be included.

65. Templates letters which prompt for the inclusion of this information will be available and will need to be adapted to the particular provisions and circumstances of the request.

66. Where the requestor wants the information electronically, the SAR response should be sent via encrypted and secure file transfer with access via a password sent to the requestor via a separate medium (typically SMS or phone call). Cryptshare is typically used for this, but other transfer mechanisms may be used provided that they have the same level of security and assurance as Cryptshare. The SAR process for the Team(s) dealing with the SAR will specify the method used for file transfer.

67. Where the requestor wants the information in hard copy, it will be sent via the following arrangements:

    a) Recorded, signed for post

    b) Courier where the information is too large to be sent via the post (usually a reem of paper is able to go via signed for delivery service). Design and Print can arrange a secure courier (cost code and delivery address details will be required).

Can requestors review files?

68. Some individuals may make a request to view their records, rather than request a copy. The Council is expected to facilitate this process.

69. If the person requests to come to a Council office to view their records, an appropriate room will be made available for viewing. At no time will the person be left un-attended. The officer accompanying the person viewing their records must be of the same gender for risk management purposes.

70. If the individual then requests copies of documents or to make a note of the documents, the standard process for sending documents should be followed.

What if the requestor is dissatisfied about the handling of their SAR?

71. A data subject may ask for a review of the way their SAR has been handled to be carried out if they believe that the provisions of the Data Protection Act have not been applied correctly in relation to:

    - what information was provided and in response to the original request;
    - any information withheld from the original response;
    - whether the Council was entitled to withhold any information from the original response;
    - whether the Council's decision to withhold information from the original response was correct in the circumstances; and
    - whether there are any factors that enable the Council to release additional information requested, either in full or in part.

72. A review will be completed by a Senior Practitioner, as identified in the relevant team's business process, within 20 working days.

73. Where the Senior Practitioner has been involved in the original SAR response, the Data Protection Officer (or their nominee) will conduct the review and respond to the requestor.

How long should SAR records be kept for?

74. With the exception of ID supplied to validate the identity of a requestor, SAR records will be destroyed 6 years after the date of creation unless there is an ongoing issue which necessitates them being retained for longer (e.g. a complaint). Records must not be retained for longer than 6 years without a documented reason.

75. ID supplied to validate the identity of a requestor will be stored with other case records relating to the SAR. A note will also be made on the case management system of what was supplied with a partial unique identifier (e.g., Driving Licence ending in xyz, Utility Bill account ending in xyz).

76. Once the information has been sent to the requester and the password has been provided, copies of the ID documents will be deleted from where they are stored.

Request for Information and Requests not covered by this procedure

<u>Adoption Records</u>

77. Records prior to someone being adopted will be processed through the SAR process. However, The SAR process is not the way in which Adopted Adults should receive information / access their records once they have been adopted.

78. The process of accessing information for an adopted adult is highly sensitive and indeed for adoptions made prior to 1975 it is a requirement that an adopted adult must undergo Birth Records counselling before accessing their information. This highlights the sensitivity and context that needs to be applied to the sharing of information and why it needs to be undertaken by a social worker with the relevant adoption experience. There is also provision in legislation to apply discretion when considering what information is shared.

79. It is very important that should requests come through for adoption records they must be referred to Adoption East Midlands (AEM) to deal with Adoption.eastmidlands@nottscc.gov.uk

Deceased persons' records

80. Deceased person's records are not covered by data protection legislation which applies to living individuals only. For this reason, the Council has a separate Deceased Person's Records Procedure Access to Deceased Persons Records Procedure.

Freedom of Information Requests

81. The Freedom of Information Act 2000 (FOIA) allows everyone the right to request access to information held by public bodies to ensure greater transparency and trust. The Environmental Information Regulations 2004 (EIR) give people the right to access environmental information from public authorities, such as information about air/atmosphere, water, soil, land and landscapes. See Freedom of Information Act (FoIA) & Environmental Information Regulations (EIR) requests.

Requests for third party personal data

82. Where the Council is sharing personal data with a third party who has requested data on a one-off basis which does not fall into the above categories, See Requests for, and disclosure of, personal information to third parties.

Roles and Responsibilities

83. All Council staff are responsible for recognising subject access requests which they may receive and understand how these requests are dealt with.

1. Specific information governance responsibilities are also allocated to individual staff members, groups and boards. The following roles have additional responsibilities around subject access requests.

    a) **Information Asset Owners (IAO)**: ensure that all assets under their control facilitate dealing with SARs. They should enable you to easily locate and extract personal data and follow retention schedule rules. They have ownership of the assets and are therefore responsible for ensuring adherence to the Data Protection principles.
    b) **Information Asset Managers (IAM)**: assist the IAOs in their role and are operationally responsible for the upkeep of information assets, including adherence to the Retention and Disposal Schedule. They also need to request and implement any changes required in accordance with this procedure.
    c) **Team / Service Managers**: ensure effective records management, such as a well-structured file plan and standard file-naming conventions for electronic documents, and monitor compliance with the Retention Schedule, whilst encouraging and working with staff to ensure ongoing compliance.

2. The **Senior Information Risk Owner** is responsible for managing information risk in the Council, ensuring information governance compliance with legislation and Council policies

3. The **Caldicott Guardian** is responsible for protecting the confidentiality of people's care information and making sure it is used properly. In this context, this means providing advice on information disclosure and confidentiality issues and being arbiter when there is a disagreement or lack of clarity on these issues.

4. The **Data Protection Officer (DPO)** is responsible for advising, monitoring, reviewing and reporting the Council's compliance with data protection legislation. The Data Protection Officer (or their nominee) will conduct SAR reviews where the senior practitioner was involved in the original SAR response.

5. The **Complaints and Information Team** will provide support and guidance in relation to this procedure.

6. The **Information Governance Team** can also provide support and guidance in relation to this procedure.

7. Relevant staff in **ICT**; **Procurement** and **relevant service areas** are responsible for ensuring that the design / purchase / acquisition IT systems and applications which process (particularly personal) information facilitate dealing with SARs and have automated records retention and deletion capabilities. **ICT** and **relevant service areas** are responsible for ensuring that, where those capabilities exist, they are deployed in line with the Records Retention and Disposal Schedule.

8. Duties assigned to specific roles referenced in this procedure must be carried out as described.

9. The Council's Information Governance Framework provides further detail of the nature of specific information governance related roles (e.g. that of SIRO, Caldicott Guardian, Data Protection Officer, Information Asset Owner, Information Asset Manager etc.) see also the intranet page on IG roles and responsibilities.

Compliance with this Procedure

10. It is a criminal offence to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information a person making a SAR would have been entitled to receive.

    You can defend this offence if you prove that:

    - the alteration, defacing, blocking, erasure, destruction or concealment of the information would have happened regardless of whether the individual made a SAR; or

- you acted in the reasonable belief that the person making the SAR was not entitled to receive the information requested.

11. Wilful or negligent disregard for information governance policies and procedures will be investigated and may be treated as a disciplinary matter under the relevant employment procedure(s) which could lead to dismissal or the termination of work agreements or service contracts.

12. It is worth noting the ICO guidance in relation to information scheduled for deletion following receipt of a SAR:
It is our view that a SAR relates to the data you held at the time you received the request. However, in many cases, routine use of the data may result in it being amended or even deleted while you are dealing with the request. So, it is reasonable for you to supply the information you hold when you respond, even if this is different to what you held when you received the request.

However, 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.

Monitoring and Review of this Procedure

13. This procedure will be periodically monitored and reviewed by the Senior Practitioner – Information, Complaints and Information Team (or their nominee) who will revise it in line with learning arising from its implementation.

14. Beyond that, the procedure will be monitored and reviewed every two years in line with legislation and codes of good practice.

Advice, Support & Further Information

15. For advice or further information on this document please contact:

The Complaints & Information Team
Email: accessto.records@nottscc.gov.uk
Telephone: 0115 9772788

16. Further reading and supporting information:

Title (as hypertext link) and publication date	Author
Complaints and Information Team SAR procedure SARS CIT Business Process.doc	Denise Maker
HR SAR procedure	

Document Control

Owner	Data Protection Officer
Author	Denise Makar, Senior Practitioner – Information and Megan Bilton, Information Governance Advisor

Last Reviewer	N/A
Approver	Senior Information Risk Owner (SIRO) under delegation from Policy Committee
Date of Approval	02/02/2023
Date of next review	02/02/2026
Version	**1.0**
Classification	Public

Version	Date	Changes and Approver