Nottinghamshire County Council

Personal Data Accuracy and Rectification Procedure

At a glance …

- Under the UK GDPR individuals can request that their personal data be corrected. Requests may be made via any channel, verbally or in writing.
- Reasonable steps must be taken to verify the requester's identity and proportionate evidence sought of the inaccuracy before making changes.
- Every request should be logged in the relevant business system (e.g. case management) and a clear audit trail maintained of actions taken.
- Requests must be acknowledged advising of next steps and timelines.
- Responses must be sent as soon as possible and within one month of receipt (extendable by up to two months for complex cases, with reasons for extension provided within the first month).
- Routine rectification requests (e.g. low-risk, undisputed, factual and requiring a simple correction) may be dealt with by the relevant service.
- Complex or contested requests (e.g. disputed facts or professional opinion, risk to integrity/meaning, implications for past decisions, shared/joint records) must be forwarded immediately to the Complaints and Information Team (C&I Team).
- When assessing a complex / contested request, the original record author should be consulted (if available) and if not, a manager / Information Asset Owner (Service Director). If needed, ultimate escalation should be to the Caldicott Guardian (social care) or the SIRO (all other records).
- Consideration should be given to restricting the processing of disputed data while checks are undertaken.
- Where information is considered accurate or reflects a justified professional view at the time, the record should not be amended. The requester should be offered a statement of disagreement to be added instead.
- Inaccuracies must be corrected with care, without deleting or obscuring the original entry. The audit trail must show what changed, when and by whom, and be annotated that the original is inaccurate.
- A record must not be altered where a Subject Access Request or court order is active. If an order covers only a specific part, unrelated corrections may proceed.
- Refusals must be justified in writing, offer a statement of disagreement and include complaint / ICO escalation routes. Only the C&I Team can issue refusals.
- Shared or multi-agency records subject to rectification requests must follow agreed governance / data-sharing arrangements.
- Where inaccurate data has been disclosed, reasonable steps must be taken to notify recipients of the rectification unless this is impossible or disproportionate.
- All outcomes must inform individuals of their right to complain via the Council's data protection complaints process and, if dissatisfied, to the ICO.

Introduction

1. Nottinghamshire County Council collects and uses personal information about residents, people who use Council services, employees and others to carry out its statutory and operational functions. The Council has a legal obligation to ensure that personal data it holds is accurate, relevant and kept up to date and makes every effort to do that.

2. Inaccurate or incomplete information can lead to incorrect decisions and may cause harm or distress to individuals.

3. Article 16 of the UK General Data Protection Regulation (UK GDPR) gives individuals the right to have inaccurate personal data rectified (made accurate).

Purpose of this document

4. This procedure sets out the steps that should be followed to ensure a consistent and effective approach is in place for managing rectification requests.

5. It forms part of the suite of documents that comprise the Council's Information Governance Framework and sits under the Information Rights Policy. It is informed by guidance provided by the Information Commissioner's Office.

6. It will be of relevance to those parts of the Council that deal with such requests, particularly the Complaints and Information Team which is responsible for managing information rights requests (including rectification requests) on behalf of the Council.

Scope

7. This procedure applies to all Nottinghamshire County Council employees, elected Members, contractors, agency workers, volunteers and temporary staff working for or on behalf of the Council.

8. It applies to all personal data created or held by the Council, in any format, including paper, electronic, email, audio and visual records, where the Council acts as Data Controller.

9. This procedure applies only to requests for rectification. Requests for access to personal information (known as Subject Access Requests (SARs)) or erasure of personal information are dealt with under separate procedures - see Subject Access Request Procedure and Personal Data Erasure Procedure (Right to Erasure).

Definitions

10. A **data controller** is a person or organisation that decides how and why personal data is collected and used.

11. **Rectification** is the process of correcting personal data that is inaccurate or incomplete, in accordance with Article 16 of the UK GDPR.

12. **Personal data** is any information relating to an identified or identifiable living individual, that is held by the Council in any format (electronic, paper, audio, visual or otherwise).

13. **Inaccurate data** is information that is incorrect, outdated, misleading or recorded in error.

14. **Incomplete data** is information that is missing details necessary to make it accurate or meaningful for the purpose for which the Council processes it.

15. A **statement of disagreement** is a note added to a record where the individual disputes the accuracy of information, but the Council concludes that the original entry should not be changed. The statement records the individual's view but does not alter the original information.

16. **Business-as-usual requests** are straightforward rectification requests involving undisputed factual errors that can be corrected by the relevant service area without forwarding to the Complaints and Information Team.

17. **Restriction of processing** is alternative safeguard where rectification investigations are (e.g. required for evidence).

Timescales

18. All rectification requests must be completed as soon as practicably possible and no later than one month from receipt. This may be extended by up to two months for complex or multiple requests, provided the individual is informed within the first month and given reasons for the delay.

19. The response clock may be paused where requester identification or request clarification reasonably needs to be obtained.

Receiving Requests

20. Requests can be made verbally or in writing and do not need to cite "rectification." They may be received by any service. Requests must be accepted via any channel and progressed without delay. Services should promptly route complex or contested requests to the Complaints & Information Team (C&I Team).

21. Where an online form is available, staff may signpost requesters to use it to ensure completeness. However, use of the form is not mandatory, and services must progress requests received by any channel without delay.

Business-as-usual requests (BAU) (handled by the service area)

22. A request may be treated as BAU where all of the following apply:

    a) The request relates to **simple factual information** (e.g. spelling errors, outdated contact information etc).
    b) The individual has provided **clear evidence** of the inaccuracy, where required.
    c) There is **no disagreement** about whether the information is incorrect.

d) The change will **not affect the integrity** of a formal record, decision, or professional judgement.
e) No legal requests for access (i.e. Subject Access Request or court order) are currently active for the same record.

23. Where BAU criteria are met, and there is confidence about the requester's identity, the service area should:

    a) update the record
    b) log the change and evidence received
    c) notify the requester of the outcome and completion date.

24. If, during processing, the case becomes contested or complex or has wider implications, it should be forwarded immediately to the Complaints & Information Team.

Complex or contested requests (handled by Complaints & Information Team)

25. A request should be forwarded immediately to the Complaints and Information Team where any of the following apply:

    a) The information in question includes a professional opinion, assessment, or judgement, and the accuracy or justification of that opinion is being challenged.
    b) Making the amendment could alter the meaning, context, or integrity of the record.
    c) The change may have consequences for previous decisions, actions, or service outcomes.
    d) The record forms part of a multi-agency, shared, or jointly controlled dataset.
    e) The request is complex, unclear, or requires further investigation.
    f) The individual indicates dissatisfaction, escalating it beyond a routine request.
    g) There is an active Subject Access Request, pre-action disclosure request, or court order covering the same record.
    h) The requester is asking for information to be deleted entirely, not just corrected.

Confirming the identity of the requester

26. Before acting on any rectification request, reasonable steps must be taken to confirm the identity of the requester to ensure that personal information is not amended on behalf of the wrong individual.

27. Where the request is made through an existing verified channel (e.g. from a known service user account or through established correspondence), further checks may not be necessary. In all other cases, appropriate identification or verification should be requested, such as proof of address, official ID, or other documentation relevant to the information being corrected. Any identity checks undertaken must be proportionate and recorded as part of the rectification audit trail.

28. Where the requester is making a rectification request on behalf of someone else, their authority to act will typically need to be checked (e.g. power of attorney).

Evidence of inaccuracy

29. When an individual requests rectification, they may be asked to provide reasonable evidence to demonstrate that the information the Council holds is inaccurate or incomplete.

30. The type of evidence required will depend on the nature of the data but may include documents such as proof of address, official identification, name-change documents, or other records relevant to the correction being requested.

31. The evidence must be assessed objectively, ensuring it is sufficient to verify the claimed inaccuracy without requesting excessive or unnecessary information. Any evidence reviewed, and the basis for agreeing or refusing the rectification, must be documented as part of the audit trail.

Logging, recording and acknowledging requests

32. All rectification requests must be logged and recorded in line with the Council's obligations under the UK GDPR. Each request should be entered into the appropriate tracking system used by the service area or the Complaints and Information Team. The record must include:

    a) the date the request was received
    b) the identity of the requester and how this was verified
    c) a description of the information the individual believes is inaccurate
    d) any other evidence provided by the requester
    e) details of any searches undertaken to verify the information
    f) the outcome of the assessment (agreed, partially agreed, or refused)
    g) dates of any amendments made
    h) copies of responses sent to the requester
    i) reasons for refusal, escalation, or any extension to statutory timescales
    j) details of any consultation with senior officers (e.g. Information Asset Owner – Service Director; Data Protection Officer; Caldicott Guardian)

33. Records should be kept in a clear and auditable format so the Council can demonstrate how decisions were reached and ensure compliance with statutory requirements.

34. Upon logging requests, a timely acknowledgment must be provided to the requester confirming that the Council has received their rectification request. The acknowledgment should:

    a) confirm the date the request was received;
    b) outline the next steps in the process;
    c) explain any requirement for further information, identity verification or supporting evidence; and

d) state the statutory timescale for responding (one month, with the possibility of extension for complex cases).

35. This ensures transparency and sets clear expectations for the individual from the outset.

Assessing and Handling Requests

36. The service area responsible for the data must firstly review the information and consider:

    a) Whether the existing data can be demonstrated to be accurate.
    b) Whether the request is routine and can be dealt with under BAU (where it meets the criteria at paragraph 22 (a – e).

37. Where the request is not routine, it should be sent immediately to the Complaints and Information Team who will work with the relevant service to determine:

    a) Whether any opinion-based information was reasonable and justified based on the information available at the time it was recorded.
    b) Whether additional evidence is required from the requester to verify the correction.
    c) Whether the person who originally recorded the information is available to give their view. If not, a manager or Information Asset Owner (service Director) should be consulted. See next section for escalation routes if required.

38. If the data is accurate or reflects a justified professional view at the time of recording, it should not be amended. The requester should be offered a statement of disagreement to be added to the record.

39. Where accuracy is contested and under review, consideration should be given to restricting processing of the disputed data until verification is complete.

Searching for information to support rectification

40. When handling a rectification request, reasonable steps must be taken to verify the accuracy of the information concerned. This may include searching relevant systems, case files, databases, emails, or archived records where appropriate.

41. Searches should be proportionate to the nature of the request but thorough enough to identify the source of the information and confirm whether it is factually correct, outdated, or recorded in error. All searches undertaken, and any evidence located, must be documented as part of the rectification record to ensure transparency and provide a clear audit trail.

Dealing with disputed or uncertain rectification requests

42. Where there is uncertainty about whether a rectification request should be agreed to, the Complaints and Information Team will gather relevant evidence and consult, if required:

- The Service Manager, Head of Service and onwards to the IAO (Service Director), if required
- The Data Protection Officer (DPO)
- The Caldicott Guardian (for social care or health-related records)
- SIRO (for all other records), where a higher-level decision is needed.

43. These senior roles will provide final oversight to ensure that borderline, disputed or complex rectification decisions are made consistently, lawfully and in a way that appropriately safeguards the individual's information rights.

44. All decisions will be evidence-based, legally justified and documented.

Amending records and protecting the audit trail

45. Council officers have a responsibility to ensure that the records they create are accurate, clear and up to date. However, errors can occur, and individuals have the right to request rectification where they believe the information the Council holds about them is inaccurate. Requests may relate to straightforward factual details (e.g. incorrect dates, spelling errors, outdated contact information etc) or disagreement with a professional assessment, observation or opinion recorded as part of service delivery.

46. Where a request relates to information that is factually accurate or reflects a justified professional view at the time it was recorded, the entry must not be amended, as doing so would compromise the integrity of the official record. In such cases, the individual should be offered the opportunity to add a statement of disagreement to the record explaining their position.

47. It is also the case that some information may have been correct at the time it was created but later became outdated as circumstances changed. This does not render the original entry inaccurate, and it should not be altered or removed.

48. Where it is agreed that information is genuinely inaccurate, it must be corrected. When amending inaccurate information, the original entry must not be obscured or deleted. The audit trail should show what was changed, when and by whom, and annotated such that the original information is inaccurate and should no longer be relied upon.

49. For paper records, inaccurate information should be struck through once, initialled, dated and with the correct details. It is important to retain readability.

50. If a Subject Access Request (SAR) or court order has been received for the full record, no part of it should be amended or deleted. If a court order relates only to a specific part, unrelated rectifications may proceed.

Refusing rectification requests

51. The Council may refuse a rectification request where there is a lawful and justified reason for doing so. The Complaints and Information Team must issue refusals and this must only be done after the request has been properly considered and relevant information has been reviewed.

Grounds for refusal

52. A rectification request may be refused where:

    a) The requester does not satisfy the Council of their identity or their authority to act for someone else who they are making a request on behalf of.
    b) The information is already accurate and the individual has not provided sufficient evidence to support the claimed inaccuracy.
    c) The request relates to a professional opinion or assessment that was reasonable and justified based on the information available at the time it was recorded.
    d) The information was correct when recorded, even if circumstances have since changed.
    e) Changing the record would compromise the integrity, meaning or audit trail of an official record.
    f) The Council is legally required to retain the original information, or deletion / amendment would conflict with statutory obligations.
    g) A Subject Access Request or legal disclosure request is currently active for the full record (in which case no changes may be made until the access process is complete).

Actions when refusing a request

53. Where a decision is made to refuse rectification:

    a) A **written response** must be sent to the requester explaining:
        - the specific reasons for refusal;
        - the evidence or justification relied upon; and
        - why the original information must remain unchanged.

    b) The individual must be informed of their right to have a **statement of disagreement** added to the record, setting out their concerns.
    c) The individual must **also be informed** of:
        - their right to complain through the Council's data protection complaints process; and
        - their right to escalate the matter to the Information Commissioner's Office (ICO) if they remain dissatisfied.

    d) The refusal decision and supporting rationale must be **fully recorded** in the case management or relevant business system.

Informing third parties

54. Where personal data has been disclosed to third parties, the Council will take reasonable steps to notify those recipients of the rectification, unless this proves impossible or involves disproportionate effort. Any notifications sent to third parties must be recorded in the appropriate case management system.

55. If requested, the individual will be informed of the recipients who have been notified.

Shared or Multi-Agency Records

56. Where personal data forms part of a shared, multi-agency, or partnership record:

    a) The approach to rectifying records must reflect the partnership governance arrangements in place (e.g. in an Information Sharing Agreement).

    b) Where partners only have view-only access, Nottinghamshire County Council (as Controller of its own dataset) will be responsible for amending information within its own system.

    c) Where a single shared system is used, responsibilities for rectification must be jointly agreed by all Controllers and set out in the relevant data sharing agreements.

57. As a rule, the organisation whose staff created the original record is responsible for making amendments.

Contracts and Third-Party Obligations

58. The Council's standard contractual terms with data processors will expressly require them to notify the Council of any request for rectification received in connection with their processing of personal data on the Council's behalf, and to cooperate fully and promptly with the Council to investigate and resolve such matters in accordance with data protection law.

59. Equivalent notification and cooperation obligations will be included in arrangements where the Council acts as a joint controller with another party, ensuring a clear allocation of responsibilities and effective coordination in responding to data subject rights requests.

Right to complain

60. If an individual is dissatisfied with the outcome of their rectification request, they must be informed of their right to complain. They may raise a complaint through the Council's data protection complaints process - information requests, personal data and privacy - in the first instance.

61. They may escalate their concerns to the Information Commissioner's Office (ICO), which oversees compliance with data protection law at any time but typically the ICO will expect the Council to be given an opportunity to complete its investigation.

62. Reference to the right to raise concerns with the ICO must be included in all responses to rectification requests, whether the request is accepted, partially accepted, or refused.

63. Complaints related to rectification requests will be handled by the Complaints and Information Team, in accordance with the Council's Data Protection Complaints Procedure.

Roles and responsibilities

64. The **Complaints and Information team** manages information rights requests received by the County Council, including responding to rights requests under the UK GDPR and the Freedom of Information Act.

65. The **Data Protection Officer (DPO)** advises on the lawful handling of rectification requests, ensures that decisions comply with UK GDPR, and provides independent oversight to safeguard individuals' rights.

66. The **Senior Information Risk Owner** provides senior oversight and assurance that rectification requests are handled lawfully, consistently and in line with organisational risk management and information governance standards.

67. The **Caldicott Guardian** provides expert oversight on the use and sharing of personal information in care settings and may be consulted on complex or sensitive rectification cases to ensure that decisions uphold confidentiality principles and protect individuals' information rights.

68. **Information Asset Owners** (Service Directors) provide oversight for rectification decisions within their directorates, resolve disputed cases in consultation with the DPO, and approve escalations to the Caldicott Guardian (social care) or SIRO (all other records) where necessary.

69. **Service Managers** are responsible for ensuring that rectification requests within their services are handled promptly and accurately, that staff follow this procedure, and that any complex or disputed cases are forwarded without delay to the Complaints and Information Team.

70. Individual **staff members** are responsible for accurately recording information, recognising and reporting potential inaccuracies, and ensuring that any rectification requests they receive are handled appropriately by either actioning straightforward corrections or promptly forwarding more complex cases in line with this procedure.

Compliance with this Procedure

71. 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.

72. Unauthorised alteration of records or failure to escalate rectification requests appropriately may also be investigated.

Monitoring and Review

73. This procedure will be reviewed as it is deemed appropriate, but no less frequently than every **three** years in line with legislation and codes of good practice.

74. Its implementation may be monitored by the Information Governance Team through its spot check programme or other mechanisms.

Advice, support & further Information

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

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

Document Control

Owner	Team Manager, Complaints and Information Team
Original Author	Caroline Agnew, Temporary IG Programme Advisor
Last Reviewer	Jason Monks, Data Protection Officer
Approver	Information Governance and Cyber Security Board (IGCSB)
Date of Approval	07/05/2026
Date of next review	07/05/2029
Version	1.0
Classification	Public

Version	Date	Changes and Approver
1.0	07/05/2026	Information Governance and Cyber Security Board (IGCSB)