

Personal Data Erasure Procedure (Right to Erasure)

At a glance ...

- Under the UK GDPR, individuals have the right to request the erasure of their personal data (“the right to be forgotten”). Requests may be made verbally or in writing and do not need to mention data protection law.
- The right to erasure is not absolute and applies only in specific circumstances.
- All erasure requests must be forwarded immediately to the Complaints & Information Team (C&I Team), who manages the process end-to-end, including identity checks, logging, assessment, actioning and communications with the requester.
- Reasonable steps will be taken to verify the requester’s identity before any action is taken. Additional proof may be required where necessary.
- The Council will respond within one month (extendable by up to two months for complex or multiple requests). The clock may be paused for ID or scope clarification.
- The C&I Team will determine whether the individual has an Article 17(1) ground for erasure (e.g. the data is no longer needed, consent has been withdrawn, the processing is unlawful, or the individual has successfully objected to the processing).
- The C&I Team will also determine whether any Article 17(3) exemption prevents deletion of the data (e.g. legal obligations, public interest / official authority tasks, archiving / research, or legal claims).
- The C&I Team will consult upon any debatable requests with relevant officers.
- Where erasure is approved, reasonable steps will be taken to identify and erase personal data across all relevant systems.
- In cases where full deletion is not technically possible (e.g. immutable backups), efforts will be made to place the data beyond use and prevented from being accessed or restored.
- Where data is held by data processors, they will be instructed, under controller – processor contracts, to erase or put data beyond use and confirm action taken.
- If the Council has shared the data, the erasure must follow existing governance and data-sharing arrangements, and the C&I Team will take reasonable steps to notify recipients and track responses.
- Where the Council has made the data public, reasonable steps will be taken (proportionate to technology and cost) to inform other data controllers.
- For direct marketing, the Council will stop marketing and place the individual on a suppression (‘do not contact’) list, to prevent future contact.
- Requests will only be refused where there is a clear and lawful rationale. A refusal must only be issued by the C&I Team and must explain the reasons, relevant exemptions, and the individual’s rights to complain to the Council and 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.
2. Article 17 of the UK General Data Protection Regulations (UK GDPR) gives individuals the right to request erasure of their personal data in defined and limited circumstances. This is sometimes known as the 'right to be forgotten.'

Purpose of this document

3. This document sets out the steps and governance requirements for handling erasure requests, ensuring compliance with the UK GDPR.
4. 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.
5. Its primary use will be the Complaints and Information Team which is responsible for managing information rights requests (including erasure requests) on behalf of the Council.

Scope

6. 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.
7. 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.
8. This procedure applies only to erasure requests. Requests for access to personal information (known as Subject Access Requests (SARs) or rectification of personal information (correction to make accurate) are dealt with under separate procedures - see [Subject Access Request Procedure](#) and [Personal Data Accuracy and Rectification Procedure](#).

Definitions

9. A **data controller** is a person or organisation that decides how and why personal data is collected and used.
10. **Erasure** is the process of permanent deletion or destruction of personal data so it is irretrievable.
11. A **data subject** is an individual whose personal data is processed by a data controller or processor.

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. **Restriction of processing** is alternative safeguard where erasure cannot be granted (e.g. required for evidence). Restriction typically means that the data can be stored but not processed further.

Timescales

14. All erasure 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.
15. The response clock may be paused where requester identification or request clarification reasonably needs to be obtained.

Receiving Requests

16. Requests for erasure may be made verbally or in writing and may be received by any part of the Council. A valid erasure request does not need to refer to “erasure,” “right to be forgotten,” “Article 17” or use any specific terminology. Any expression of a wish to have personal data deleted must be treated as a right to erasure request.
17. All staff must recognise erasure requests and forward them immediately to the [Complaints & Information Team](#) (C&I Team). Service areas must not attempt to determine eligibility or action deletion themselves. This ensures consistency, legal accuracy, and appropriate consideration of exemptions.
18. Where an online form exists, staff may signpost the requester to it to assist completeness. However, use of the form is not mandatory, and requests cannot be delayed or refused because the individual has not used a particular channel.

Confirming the identity of the requester

19. Before acting on any erasure request, reasonable and proportionate steps must be taken to confirm the identity of the requester, ensuring that personal data is not deleted in error or at the request of an unauthorised party.
20. Where the request is made through an existing trusted channel (e.g. ongoing casework with verified identity), further checks may not be necessary. In all other cases the C&I Team will coordinate appropriate identity checks.
21. Where a request is made on behalf of another individual, evidence of authority to act (e.g. power of attorney) must be obtained. All identity verification activity must be logged by the C&I Team.

Logging, recording and acknowledging requests

22. Upon receipt, the C&I Team must log all erasure requests in the appropriate case management system. Records should demonstrate due diligence and accountability and must include:
- a) Date the request was received
 - b) How identity was verified
 - c) Description of the data that the data subject wants erasing
 - d) Systems and repositories likely to contain the data (focus of the search)
 - e) Whether any third-party sharing has occurred
 - f) The assessment of applicable Article 17(1) grounds and Article 17(3) exemptions
 - g) Actions taken and dates
 - h) Communications with the requester and any third parties.
23. Within a month of receiving the erasure request, the C&I Team will issue a timely acknowledgment confirming receipt, explaining the next steps, the statutory one-month timescale (and possibility of a two-month extension where the request is complex or involves multiple requests), and noting any need for identity verification or clarification.

Assessing requests

24. The C&I Team leads on the assessment of every erasure request. The right to erasure is **not absolute** and must always be balanced with the following exemptions. The assessment of a request must consider:

Whether a ground under Article 17(1) applies

25. Individuals have the **right to have their personal data erased if**:
- a) The personal data is no longer needed for the original purpose it was collected or processed for (for instance, where the Council's [Records Retention and Disposal Schedule](#) indicates that the data has been held beyond the stated retention period without a legitimate reason).
 - b) The Council is relying on the individual's consent as the lawful basis for processing the data, the consent is withdrawn and no other lawful basis exists.
 - c) The Council is relying on the legitimate interests as the lawful basis for processing the data, the individual objects to processing and there are no overriding legitimate grounds to continue the processing.
 - d) The personal data is being unlawfully processed.
 - e) Erasure is required to comply with a legal obligation.
 - f) The data was processed in relation to information society services offered to a child.
 - g) the personal data has been processed as a result of an allegation about the data subject:
 - i. which was made by a person who is a malicious person in relation to the data subject;
 - ii. which has been investigated by the data controller; and

- iii. in relation to which the controller has decided that no further action is to be taken.

26. In respect of clause 17g(i), a new Article 17(4) of the UK GDPR defines a “malicious person” as someone convicted of a specified offence or subject to a stalking protection order. This includes individuals guilty of harassment or subject to stalking orders where the data subject is the victim. The provision allows victims to request erasure of their personal data where it was processed because of an unfounded allegation made by their perpetrator.

Whether any exemptions under Article 17(3) apply

27. The right to erasure **does not apply** if processing is necessary for one of the following reasons:

- a) For exercising the right of freedom of expression and information.
- b) For compliance with a legal obligation (i.e. if another law requires you that the data be retained such as employee records under employment or health and safety law).
- c) For the performance of a task carried out in the public interest or in the exercise of official authority (i.e. performing public functions and powers that are set out in law or performing specific tasks in the public interest that are set out in law)
- d) For archiving in the public interest, scientific / historical research or statistical purposes where erasure would impair processing objectives.
- e) For the establishment, exercise or defence of legal claims (e.g. potential tribunal claims by an employee or potential contract disputes or negligence claims by customers or suppliers).

28. The UK GDPR also specifies two circumstances where the right to erasure will not apply to **special category data**:

- a) For reasons of public health purposes in the public interest.
- b) For purposes of preventative or occupational medicine, assessing an employee's working capacity, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services, where the processing is carried out by, or under, the responsibility of a health or social care professional who is legally bound by a professional duty of confidentiality.

Whether restriction is required instead of erasure

29. Where erasure cannot be granted immediately (e.g. because data is subject to a legal hold, is needed to defend claims, or deletion is not feasible in backup environments) the C&I Team must consider restricting the data (i.e. under a restriction data will be stored but not used).

Actioning an erasure

30. Once the C&I Team has confirmed that the requester has a ground apply for erasure and no exemption prevents erasure of their data, the following steps will be taken to action the request:

Searching for information to support erasure

31. Before any erasure activity can take place, the C&I Team will identify all locations where the personal data is held. Searches will be proportionate yet comprehensive and will include, where relevant, live systems, archived records, cloud platforms, email, shared network drives, physical records, and backup environments.
32. In coordination with the relevant service area, system owners, IT colleagues and (where applicable) partner organisations, the C&I Team will map all instances of the data so that complete erasure, or the application of “beyond use” controls, can be carried out. All search activity will be documented.

Erasing data from live systems

33. Where technically possible, data will be securely and permanently deleted from all live systems. This includes application databases, shared drives, email accounts, document stores and case management systems. Erasure must ensure the data cannot be reconstructed or accessed.

Dealing with backups and technical limitations

34. If data cannot be erased from backups or legacy systems due to technical constraints, the Council will make efforts to apply a “beyond use” safeguard. This means:
 - no attempt will be made to access the data;
 - the backup will not be restored except in disaster recovery; and
 - if restored, the data will be deleted at that point.
35. Individuals must be informed where their data has been put “beyond use” and how it applies.

Notifying processors

36. Where a third-party processor holds data on the Council’s behalf, the C&I Team will liaise with the relevant service and / or legal services and issue instructions in accordance with controller–processor contractual requirements, to ensure erasure or “beyond use” controls are applied by the processor. Confirmation of completion will be requested.

Direct marketing: suppression instead of deletion

37. Where the request relates to direct marketing data, the Council will stop all marketing activity and place the individual’s details onto a suppression (“do not contact”) list, rather than delete them. This ensures the Council does not inadvertently contact the individual again, in line with ICO guidance.
38. A suppression entry is not further processed for marketing purposes and exists solely to prevent future contact.

Informing third-party recipients

39. Where the Council has shared the individual's personal data with other organisations, the C&I Team will take reasonable steps to notify those recipients that erasure has been approved, so they can erase the data in their systems.
40. The C&I Team will keep a record of the data recipients notified and, if notification is not reasonably possible, the reason(s) why. The individual will be informed of the recipients to whom the erasure notification was sent, where they request this information.
41. Where the Council has made personal data public, the C&I Team will, taking account of available technology and proportionality, take reasonable steps to inform other controllers processing the data that the individual has requested erasure of any links, copies or replications.

Shared or multi-agency records

42. If the personal data forms part of a shared, multi-agency or partnership record, the approach to erasure, including notifying of a request, must follow the governance arrangements in the relevant information sharing agreements or joint controller agreements (e.g. rules for initiating, actioning and confirming erasure).
43. The C&I Team will coordinate with partner controllers and any processors to ensure that erasure (or "put beyond use" where applicable) is completed consistently across the shared environment and that audit trails are maintained.
 - Where partners have view-only access to Council-held data, the Council will erase data in its own systems and notify partners where appropriate.
 - Where a single shared system is used, responsibilities for erasure and notification will be applied as set out in the partnership agreement; if not specified, the C&I Team will liaise with partner controllers to agree a practical approach and timescales.
44. All notifications and confirmations must be recorded by the C&I Team. Outcome letters to individuals will state that relevant recipients have been notified (or explain why this was not reasonably possible).

Confirming completion

45. The C&I Team will ensure that all deletions and "beyond use" actions are completed and recorded. A final response will be issued to the requester, explaining the actions taken, any limitations (e.g. backups), and their right to complain to the Council and / or the ICO.

Dealing with disputed or uncertain erasure requests

46. Where there is uncertainty about whether erasure is required (e.g. because of possible legal obligations, safeguarding implications, or legitimate interests) the C&I 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.

47. 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.

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

Refusing erasure requests

49. The Council may refuse an erasure request where there is a lawful and justified reason for doing so. The C&I 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

50. An erasure request may be refused where:

- a) No Article 17(1) condition applies
- b) An Article 17(3) exemption applies
- c) The request is manifestly unfounded or excessive (in line with criteria issued by the Information Commissioner's Office).

Actions when refusing a request

51. Where a decision is made to refuse an erasure request:

- a) A **written response** must be sent to the requester explaining:
 - the specific reasons and legal basis for the refusal
 - any alternatives that that can be offered (e.g. restricting the data) and what this means in practice
- b) 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.
- c) The refusal decision and all supporting evidence must be **fully recorded** in the case management system.

Contracts and Third-Party Obligations

52. The Council's standard contractual terms with data processors will expressly require them to notify the Council of any request for erasure 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.
53. 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

54. If an individual is dissatisfied with the outcome of their erasure, 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.
55. 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.
56. Reference to the right to raise concerns with the ICO must be included in all responses to erasure requests, whether the request is accepted, partially accepted, or refused.
57. Complaints related to erasure requests will be handled by the Complaints and Information Team, by a separate officer who dealt with the original request, in accordance with the Council's [Data Protection Complaints Procedure](#).

Roles and responsibilities

58. 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.
59. The **Data Protection Officer (DPO)** advises on the lawful handling of erasure requests, ensures that decisions comply with UK GDPR, and provides independent oversight to safeguard individuals' rights.
60. The **Senior Information Risk Owner** provides senior oversight and assurance that erasure requests are handled lawfully, consistently and in line with organisational risk management and information governance standards.
61. 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 erasure cases to ensure that decisions uphold confidentiality principles and protect individuals' information rights.
62. **Information Asset Owners** (Service Directors) provide oversight for erasure 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.

63. **Service Managers** are responsible for ensuring that all erasure requests received within their service are promptly forwarded to the Complaints and Information Team, and they may provide operational insight where needed to support the assessment of how the erasure request should be handled.
64. Individual **staff members** are responsible for recognising erasure requests and promptly forwarding them to the Complaints and Information Team. They may also assist in identifying systems and records containing relevant data.
65. **IT / System Administrators** support technical erasure, ensure backups are put beyond use where immediate deletion is not feasible, and confirm secure destruction.

Compliance with this Procedure

66. 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.
67. Unauthorised alteration or deletion of records or failure to escalate erasure requests appropriately may also be investigated.

Monitoring and Review

68. 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.
69. Its implementation may be monitored by the Information Governance Team through its spot check programme or other mechanisms.

Advice, support & further Information

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

The Complaints & Information Team
Email: accesstorecords@nottsc.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)