

Data Protection Complaints Procedure

At a glance ...

- The Data (Use and Access) Act 2025 requires the Council to provide a clear and accessible way for people to raise concerns about how their personal data is handled.
- This procedure explains how the Council will receive, triage, investigate, respond to and learn from data protection complaints.
- Individuals will typically be expected to raise their concerns with the Council first, before approaching the Information Commissioner's Office (ICO).
- Complaints can be submitted online (via an online form), by post, or by telephone.
- Two Council teams handle complaints:
 - The Complaints & Information Team (C&IT) handles complaints relating to information rights, including Subject Access Requests (SARs) and other statutory rights.
 - The Information Governance (IG) Team handles complaints about all other aspects of data protection, including reports of personal data breaches and other alleged data protection infringements
- Complaints will be acknowledged promptly and within 30 days, investigated proportionately and fairly, and concluded without undue delay, normally within three months.
- Complainants will receive a clear written outcome explaining the findings, actions taken, and how to escalate to the ICO if they remain dissatisfied.
- All complaints are logged, analysed and reported, with trends and learning fed into improvement actions across the Council.
- This procedure supports the Council's Information Governance Framework and related policies, including the Information Rights Policy, Data Subject Rights Procedure, and Data Security Incident & Breach Management Procedure.

Introduction

1. Nottinghamshire County Council is committed to protecting people's personal information and complying with data protection law. The Data (Use and Access) Act 2025 requires all organisations to provide a clear and accessible way for individuals to complain about how their personal data is handled.
2. Under the Act, individuals are expected to raise their data protection complaint with the Council first, and the Council must operate a formal complaints process to handle it. This

gives the Council the opportunity to resolve the matter, before the individual exercises their right to then escalate to the Information Commissioner's Office (ICO) (the UK data protection regulator).

3. The Council may be required to report to the ICO the number of complaints (and potentially other information if required by future regulations).

Purpose of this document

4. This procedure sets out how Nottinghamshire County Council will maintain and operate a formal data protection complaints process, as required by the law and following guidance from the ICO.
5. It explains how individuals can raise complaints about the Council's handling of their personal information and how the Council will acknowledge, investigate, respond to and learn from those complaints.
6. It forms part of the County Council's [Information Governance Framework](#) and sits under the [Information Rights Policy](#) and [Data Subject Rights Procedure](#).

Scope

7. This procedure applies to all staff and elected members including employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information.
8. It applies to all personal information for which the Council acts as data controller, or joint Data Controller.
9. It does not cover non-data protection complaints, which are managed under [corporate complaint's procedures](#). However, both the data protection and corporate complaints procedures will cross-reference to each other, and complaints will be handed over between the two processes where the nature of the complaint necessitates (e.g. a corporate complaint that also includes an alleged data breach).

Definitions

10. A **data controller** is a person or organisation that decides why and how personal data is collected and used.
11. A **complaint** is any expression of dissatisfaction or concern relating to the Council's handling of personal data or compliance with data protection legislation. This includes:
 - a) reports of alleged personal data breaches from or on behalf of the individual(s) affected;
 - b) requests for internal review of the Council's handling of data subject rights (e.g. Subject Access Requests); and
 - c) concerns about how the Council has collected, used, shared, retained or otherwise processed personal information.
12. A **complainant** is the person making the complaint.

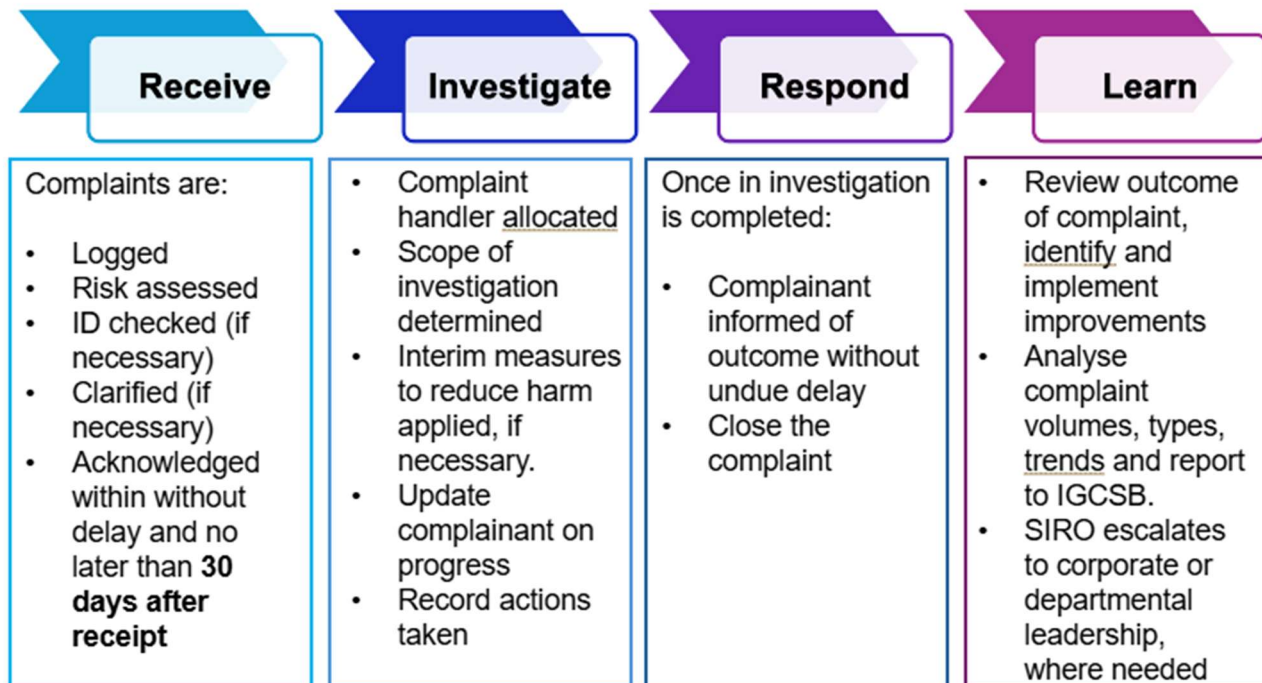
Principles & Commitments

13. The Council aims to ensure complaints are acknowledged promptly, investigated fairly and thoroughly, and resolved without undue delay.
14. The following principles will be applied to the complaints process:
- a) **Accessibility:** there will be simple, accessible routes to lodge a complaint.
 - b) **Proportionality:** investigations will be commensurate with the nature, scope and risk to the complainant.
 - c) **Timeliness:** complaints will be **acknowledged as soon as possible and no later than 30 days**; progress updates will be provided where investigations are likely to take longer than originally communicated to the complainant; and the **outcome of the complaint will be communicated without undue delay and will typically not take longer than three months**.
 - d) **Transparency:** communications will be plain language with clear explanations of findings and actions.
 - e) **Accountability and learning:** complaints will be recorded, analysed for trends, reported and be used to instigate and embed improvements.
15. Individuals can raise a complaint by using any of the following channels:
- a) **Online:** Complete the Data Protection Complaint Form - [Information requests, personal data and privacy | Nottinghamshire County Council](#) on the Council's website.
 - b) **Post:** Data Protection Officer, Nottinghamshire County Council, County Hall, Nottingham NG2 7QP.
 - c) **Telephone:** 0300 500 80 80
16. This procedure will be available on the Council's public website. Links to it and the complaints form will be prominently displayed on privacy notices and relevant webpages.
17. Privacy notices will inform individuals that they may raise a data protection complaint with the ICO at any time. However, the ICO generally expects organisations to have been given the opportunity to address the issues raised before individuals contact them. **Appendix A** contains indicative standard wording, relating to the complaints procedure to be used in privacy notices.
18. Personal data breaches reported by individuals affected will be treated as data protection complaints from the point of receipt. The Council will continue to manage and record all personal data breaches in line with the Data Security Incident & Breach Management Procedure. Where appropriate, the Council may offer an internal review of its breach response in accordance with that procedure.

Responsibilities, Process, Overview and Timeframes

19. The Complaints and Information Team (C&IT) will be responsible for the complaints process relating to information rights, the Information Governance Team will be responsible for all other types of data protection complaints.

20. The following is an overview of the data protection complaints procedure.



Detailed Procedure and Timeframes

21. The following provides more detail of the procedure.

Receiving and triaging a complaint

22. On receipt, the Complaints and Information Team (for information rights complaints) and the IG Team (for all other data protection complaints) will log the complaint, give it unique reference and categorise it (e.g. Subject Access Request handling, personal data breach, data retention, profiling, lawful basis for processing personal data, data sharing etc).

23. Steps will be taken to verify the identity of the complainant where appropriate.

24. If clarification is needed to understand the scope for the complaint, it will be requested promptly.

25. Where it is unclear what a complaint is about, the complainant will be asked for more information as quickly as possible. The complainant will also be asked what outcome they're looking for. For example, do they want a decision that has been made to be altered, an apology for a mistake, or change of process or procedure. This may help to narrow the scope of the investigation and resolve the complaint more quickly.

26. Triage determines whether the matter relates solely to data protection or also requires parallel handling under the corporate complaints policy. Where that is the case, details will be forwarded through the relevant complaints process.

Acknowledging a complaint

27. The complaints will be acknowledged immediately and confirmed in writing as soon as possible and no later than 30 days after receipt, with the complainant being given a unique reference number for the complaint.

28. Different acknowledgement methods may be used depending on how the complaint was received:

- a) Verbal complaints will be recorded and followed up in writing within 30 days after being received.
- b) Electronic complaints (e.g. through email or live chat) could use an automatic response. Where a complaint is received via social media, The Council will move the discussion to a more secure channel (email, portal or post) for identity verification and information security.
- c) Written complaints will be followed up with an acknowledgement letter.

29. An indicative template acknowledgement letter can be found at **Appendix B**.

Investigating a complaint

30. Where a complaint takes the form of a request for internal review (for example, in relation to a data subject rights request), the investigation will focus on the handling of the original request.

31. Where the complaint relates to a reported personal data breach, it will be investigated as a data protection complaint in accordance with this procedure, drawing on the Council's Data Security Incident & Breach Management Procedure as appropriate. Any internal review of the breach response is managed separately in line with that procedure.

32. The allocated complaint case handler from the C&I or IG teams, as appropriate, will define the investigation scope, evidence sources, stakeholders to consult, and milestones. The complaints handler will not have worked on any aspect of the personal information processing that has given rise to the complaint.

33. An appropriate level of enquiries will be made to be able to justify why a complaint was handled in a particular way.

34. The investigation will gather as much information as needed, including:

- a) looking at all the relevant facts thoroughly, fairly and accurately;
- b) speaking to relevant members of staff;
- c) reviewing audit logs,
- d) comparing the information from the complaint with the information held by the Council; and
- e) checking that the Council has upheld its own terms, policies and standards.

35. Interim measures (e.g., stopping a processing activity, applying additional safeguards, accelerating a SAR response) may be taken where appropriate to reduce harm.
36. The complainant will be updated on the progress of the investigation. If the investigation is likely to take some time, the acknowledgement of receipt of the complaint should be followed up so the complainant knows work is underway to resolve the issue. It may be appropriate to provide them with a date the investigation is expected to be completed and a point of contact if they have questions.
37. Having an open dialogue with complainants can build trust and lead to people making fewer complaints to the ICO, before the Council has had the opportunity to address concerns and / or put things right.

Recording actions taken

38. The case handler will document facts, applicable law, risks to the individual, and any breach of policy or law.
39. Records to be held in support of the complaint will include:
- a) the complaint and the date it was received.
 - b) the complaint acknowledgement and the date it was sent;
 - c) any relevant correspondence and document including notes of conversations, investigation notes, evidence reviewed
 - d) the outcome of the complaint and the date it was sent;
 - e) any actions taken as a result of the investigation.
40. Data protection complaint records will be retained in line with the Council's [Records Retention and Disposal Schedule](#). Access will be restricted to authorised staff.

Informing the Complainant of Outcome

41. Having completed the investigation, the C&I or IG team will let the complainant know the outcome, as soon as possible and without undue delay.
42. The outcome communication will clearly explain what has been done to resolve the complaint and, where appropriate, any actions taken as a result. Sufficient information and evidence will be included to help the complainant understand how the conclusion has been reached.
43. To achieve this the outcome letter will be written in plain language, setting out:
- a) summary of the complaint
 - b) the investigation steps taken
 - c) findings
 - d) actions taken and planned
 - e) information about the right to escalate to the ICO and how to do so; and
 - f) contact details for further questions

44. If the complaint is upheld, the letter will include the Council's remedial steps and timescales. Where not upheld, the Council will explain the reasons and any improvements identified.
45. Where applicable, the outcome will explain any further options available, including internal review mechanisms relevant to the type of complaint.
46. The complainant will be advised that they have the right to complain to the ICO.
47. An indicative template outcome letter can be found at **Appendix C**.

Closing a complaint

48. Following closure, the Complaints and Information or IG team will record the resolution, categorise the outcome, and log improvement actions on the Data Protection Complaints Register. There may need to be some follow-up to ensure that improvement actions planned have been completed.

Learning and reporting complaints

49. Once an outcome has been provided to the complainant, there will be a review of the specifics of what happened. This will consider if there is anything can be learned or improved on to prevent future such complaints.
50. A quarterly report summarising volumes, categories, timeliness of resolution, nature of resolution and trends of data protection complaints will be submitted to the Information Governance and Cyber Security Board by the Data Protection Officer. The Report will offer recommendations on any actions that need to be taken to reduce to complaints, together with an owner and date for completion.
51. The Senior Information Risk Owner, who is chair of the Board, will decide whether any significant risks, issues, trends identified are escalated to corporate or departmental leadership teams (as appropriate), with proposed actions and timelines for resolution (e.g. policy or process updates, additional training / communication or audits etc).
52. The ICO may require the Council to report to the ICO the number of complaints (and potentially other information if required by future regulations).

Resourcing the complaints process

53. The Council will take steps to ensure the data protection complaints process is adequately resourced by suitably trained staff.
54. These staff will work in the Complaints and Information Team for complaints related to information rights and the IG Team for complaints associated with other areas of data protection law (e.g. personal data breaches etc).

Training and Awareness

55. All Council staff should be able to recognise when a concern raised by an individual relates to the handling of their personal data. A data protection complaint may not

always be labelled as such; it could appear in correspondence, phone calls, or face-to-face discussions about issues like delays in SAR responses, incorrect data, or perceived misuse of information.

56. Training will be provided to all staff as part of annual data protection training to help them identify data protection complaints and understand the escalation route. Staff should signpost complainants to the published complaints page and privacy notices, ensuring the route is easy to find.
57. Training will be augmented by periodic awareness raising and up to date information on the Council's [Data Protection and Information Governance intranet hub](#).

Contracts and Third-Party Obligations

1. The Council's standard contractual terms with data processors will expressly require them to notify the Council of any data protection complaint 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.
2. 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 protection complaints.

Roles and Responsibilities

58. The **Data Protection Officer (DPO)** is accountable for the procedure, oversight of complex cases, decision-making on legal issues and exemptions, reporting to the Information Governance and Cyber Security Board, and engagement with the ICO if needed.
59. The **Senior Information Risk Owner** will decide whether significant risks or systemic issues associated with data protection complaints are escalated to corporate or departmental leadership, with proposed actions and timelines for resolution.
60. Where a complaint involves the handling, sharing, or protection of personal confidential social care information, the **Caldicott Guardian** may be consulted to provide expert oversight on whether data use or disclosure was necessary, proportionate, lawful, ethical, and in line with the Caldicott Principles.
61. The **Complaints and Information team** operates the process for complaints related to data subject rights.
62. The **IG team** operates the complaints process for other areas of data protection including data breaches, fair processing etc.
63. **Service Managers** provide evidence and responses within agreed timeframes; implement remedial actions and improvements.

64. **ICT** and **Data Owners** provide system access, audit logs and technical information; implement technical controls or configuration changes, where necessary.

Compliance with this Procedure

65. Wilful or negligent disregard for information governance policies, procedures and standards 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 agreement or service contracts.

Procedure

66. This Procedure will be periodically monitored and reviewed by the Data Protection Officer (or their nominee) who will revise it in accordance with any learning arising from its implementation.

67. Beyond that, the Procedure will be monitored and reviewed every three years considering legislation and codes of good practice.

Related legislation

68. Related legislation includes:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Data (Use and Access) Act 2025

Related Council policies

69. Related County Council policies and standards include:

- [Information Rights Policy](#)
- [Data Subject Rights Procedure](#)
- [Subject Access Request procedure](#)
- [Data Security Incident & Breach Management Procedure](#)

Advice and Support

70. Further advice about this procedure can be obtained from:

Information Governance Team

Email: data.protection@nottsgov.uk

Telephone: 0115 80 43800

Document Control

Owner	Data Protection Officer
Original Author	Caroline Agnew, Temporary IG Programme Advisor

Last Reviewer	Jason Monks, Data Protection Officer
Approver	Information Governance and Cyber Security Board
Date of Approval	25/06/2026
Date of next review	24/06/2029
Version	1.1
Classification	Public

Version	Date	Changes and Approver
1.0	07/05/2026	Approved by Information Governance and Cyber Security Board
1.1	25/06/2026	Approved by DPO. Updated to clarify the classification of data protection complaints, including the treatment of data subject-reported breaches and requests for internal review, and to align with the Data Security Incident & Breach Management Procedure.

Indicative wording for Council privacy notices

Data Protection Complaints

If you have concerns about the way Nottinghamshire County Council has collected, stored, shared or otherwise used your personal data, please provide details of by:

Completing our online Data Protection Complaint Form available at [Information requests, personal data and privacy | Nottinghamshire County Council](#)

Telephoning: 0300 500 8080

Writing to:

The Data Protection Officer
Nottinghamshire County Council
County Hall
Nottingham
NG2 7QP

Contacting the Information Commissioner's Office

You can seek advice and have the right to make a complaint to the Information Commissioner's Office. The ICO is an independent body set up to uphold information rights in the UK.

Please note though that the ICO usually expects you to raise the matter with us first so that we have the chance to resolve it.

You can contact the ICO through the [Information Commissioners Office](#) website, their helpline on 0303 123 1113, or in writing to:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire,
SK9 5AF

Complaint Acknowledgement - Indicative Template

Subject: Your Data Protection Complaint – Acknowledgement (Ref: [Ref])

Dear [Name],

Thank you for contacting Nottinghamshire County Council about our handling of your personal information. We have logged your complaint under reference [Ref], received on [Date].

An Information Governance case handler will investigate your concerns. We aim to keep you updated during our enquiries and to provide an outcome without undue delay. Our planning benchmark is to resolve most complaints within three months.

If we need any further information (for example, identity verification or clarification of the scope of your complaint), we will contact you promptly.

If you have any questions, please email INSERT or call INSERT.

Kind regards,
INSERT
Nottinghamshire County Council

Outcome Letter – Indicative Template

Subject: Outcome of Your Data Protection Complaint (Ref: [Ref])

Dear [Name],

Thank you for your patience while we investigated your complaint about how Nottinghamshire County Council handled your personal information.

Summary of your complaint:

[Set out, in plain language, the concern]

Investigation steps:

[Summarise enquiries, evidence sources and consultations]

Findings:

[Explain what we found]

Actions taken / planned:

[Describe remedial steps and timescales, or reasons if no breach found]

Next steps and escalation:

We hope that this response addresses the concerns you raised. However, if you remain dissatisfied, you may raise your concerns with the Information Commissioner's Office (ICO)

Website: [Information Commissioners Office](#)

Helpline on 0303 123 1113,

Or in writing to:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire,
SK9 5AF

If you have questions, please reply to this email or contact the [Name] Team on email [\[details\]@nottsc.gov.uk](mailto:[details]@nottsc.gov.uk) or call [number].

Kind regards,

[Name]

[Title]