Nottinghamshire County Council

Information Sharing Agreement (ISA) Procedure

At a glance …

- Information sharing with external organisations can be hugely beneficial in helping the Council and its partners to achieve better outcomes for individuals and communities.
- Data protection law does not prevent information sharing but provides a framework to ensure it is done lawfully, proportionately, and appropriately.
- Information Sharing Agreements (ISAs) are a key means of ensuring that routine sharing of personal data with external organisations is properly considered and securely executed. All such sharing must have an ISA.
- ISAs are formal agreements that describe the terms and conditions for sharing personal information.
- A Summary (and maybe a full) Data Protection Impact Assessment (DPIA) will be required to assess risk to individuals of the sharing and inform the ISA.
- Council initiated ISAs should use the corporate ISA template.
- The Information Governance (IG) Team will support the Information Asset Owner (or their nominee) through the DPIA and ISA process.
- The IG Team will maintain a register of ISAs to which the Council is a signatory. Information Asset Owners and Managers must let the IG Team have a copy of all ISAs.
- The Data Protection Officer (or their nominee) will be consulted during the drafting of an ISA and associated DPIA in order to provide advice.
- ISAs will be authorised for sign-off by either the Information Asset Owner; Caldicott Guardian or the Senior Information Risk Owner (SIRO) depending on the data being shared.
- All ISAs will have a Council nominated Single Point of Contact (SPoC) who will handle queries and periodically (no less than every two years) review sharing arrangements. ISAs will typically last no longer than six years.
- Until an ISA is signed-off relevant data should not be shared.
- If there is a material change in the way the sharing operates (e.g. introduction of new technology or a widening of scope etc) a new / refreshed DPIA / ISA maybe required, and advice should be sought from the IG Team.
- This procedure does not cover ad hoc / one off disclosures of information (e.g. to the police or solicitors); Freedom of Information Requests; Subject Access Requests. In these cases, see guidance on disclosing information.
- ISA numbers and related risks and issues will be reported to the Information Governance and Cyber Security Board.

Background

1. The County Council collects and uses huge volumes of personal data to provide quality services to communities, businesses, and individuals. It is responsible for ensuring that information is used in ways which comply with human rights, data protection and other relevant legislation.

2. Data sharing across and between organisations can bring significant benefits. Done well, it can help to design and deliver modern, efficient services which better meet people's needs and make their lives easier. It can also identify people at risk and address problems before they have a significant adverse impact.

3. Data protection does not prevent data sharing but creates a framework within which it can be undertaken in a lawful, appropriate, and proportionate way which balances organisational needs with the rights of individuals.

4. Information Sharing Agreements (ISAs) are a key means of ensuring that routine sharing of personal data is properly considered and securely executed.

5. Organisations which do not comply with or cannot evidence compliance with data protection legislation can be subject to very significant fines.

Purpose

6. This document sets out Nottinghamshire County Council's procedure for conducting and agreeing ISAs

7. It forms part of the suite of documents that comprise the Council's Information Governance Framework and is a requirement of the Information Compliance Policy. The Information Compliance Policy commits that the Council will apply this policy and good information governance to all our work and the information we handle, in recognition of our duty to the public as well as complying with legislation.

Scope

8. This procedure applies when the Council initiates sharing (or receives a request to share) personal data on a regular basis with an external body.

9. It applies to systematic information sharing, described by the Information Commissioner's Office as '*routine sharing of data sets between organisations for an agreed purpose'*. It will also apply where a group of organisations arrange to 'pool' their data for specific purposes. In these instances, the information sharing will typically require an ISA.

10. This Procedure does not apply to information sharing between the Council and its suppliers, where the supplier is processing personal data on the Council's

behalf. In this situation the supplier is classed as a data processor, and the law requires that a written contract must be in place between the Council and processor in order to protect the rights of the individuals whose data is being processed. The contract will include a data processing agreement setting out why and how the data will be processed. An ISA is typically not required.

11. This Procedure does not apply to the sharing of personal information between teams within the Council as an Information Sharing Agreement is not required for this. However, data protection principles are that data should only be used for the purposes for which it was collected and must not be used for incompatible purposes. Therefore, any internal sharing of personal data needs to be undertaken in line with this principle and on a need to know basis. It is recommended that the Internal Data Sharing form (available in the Data Protection and Information Governance intranet hub) completed to document the rationale behind any such sharing.

12. There are occasionally residual data sharing / transfer issues between the Council and its Alternative Service Delivery Models (ASDMs) – Via, Arc and Inspire etc. A separate process has been put in place to deal with this matter. A form has been devised to document and authorise this type of data sharing / transfer. Further details are available from the Information Governance Team.

13. The safeguarding of children or vulnerable adults will take precedence over data protection law in (typically one-off) situations where not sharing the data may present a risk of harm to individuals. However, in these situations, privacy considerations should be made, risks assessed, and decisions documented.

14. Ad hoc, one off requests for information from third parties (such as the police, courts and other local authorities) should be dealt with in accordance with the Council's guidance on disclosure of personal information to third parties.

15. This procedure does not apply to statutory requests for information (such as Freedom of Information requests, Subject Access requests or Environmental Information requests (which are covered by separate procedures). See guidance on requests for, and access to, information.

16. Requests from individuals or their representatives for access to, or copies of, their personal data, will be referred to the Complaints & Information team and handled as a Subject Access Request.

17. Deceased persons data is not classed as personal data for the purpose of data protection law but is covered by Human Rights legislation and as such an ISA may still be required. The Council has produced guidance on sharing deceased persons' records, and advice on sharing this data should be sought from the Complaints and Information Team..

18. This procedure applies to all staff including: employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information.

Definitions

19. Reference to information and data in this procedure is used as a collective term. The focus is on personal data, although the same considerations may apply to the sharing of other sensitive data, for example commercially sensitive information.

20. Personal data is any information relating to a living identified or identifiable person which may directly or indirectly identify them.

21. Information can be in any format including paper, electronic, digital images, voice recordings etc. Processing of information includes anything you might do with it.

22. A data controller is an individual or organisation which determines how and why personal data is being processed. A data processor processes personal data on behalf of a data controller.

23. A data subject is defined as an identified or identifiable individual to whom personal data relates.

24. ISAs are formal agreements that describe the terms and conditions for sharing personal information. They document the purpose and standards of the data sharing; roles and responsibilities of the parties involved and are an important measure of documenting accountability and compliance with the law.

25. Data Protection Impact Assessments (DPIAs) are a means for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal data and for evidencing the mitigation of those risks.

Principles & Commitments

26. The Council has committed that any information sharing is undertaken confidentially, securely, lawfully and consistently and that Information Sharing Agreements (ISAs) are in place where considered necessary.

27. All routine personal data sharing should have an ISA in place between the parties. Information Asset Owners are accountable for ensuring that this is done whereas Information Asset Managers are responsible.

28. A Data Protection Impact Assessment will typically be required to assess risk to data subjects of routine personal data sharing and inform the drafting of Information Sharing Agreements.

29. ISAs initiated by the Council will be assigned a Single Point of Contact (SPoC) within the service sharing data who will be referenced in the ISA and be available to handle queries related to the information sharing covered.

30. For the ISAs which it initiates, the Council will have an ISA template which has been developed by legal services and which follows relevant codes practice for information sharing, particularly that of the Information Commissioner's Office.

31. The Council's Information Governance (IG) Team will maintain a register of ISAs to which the Council is a party. This will include ISAs initiated by the Council or third parties. It is the responsibility of Information Asset Owners and Information Asset Managers to ensure ISAs are shared with the IG Team.

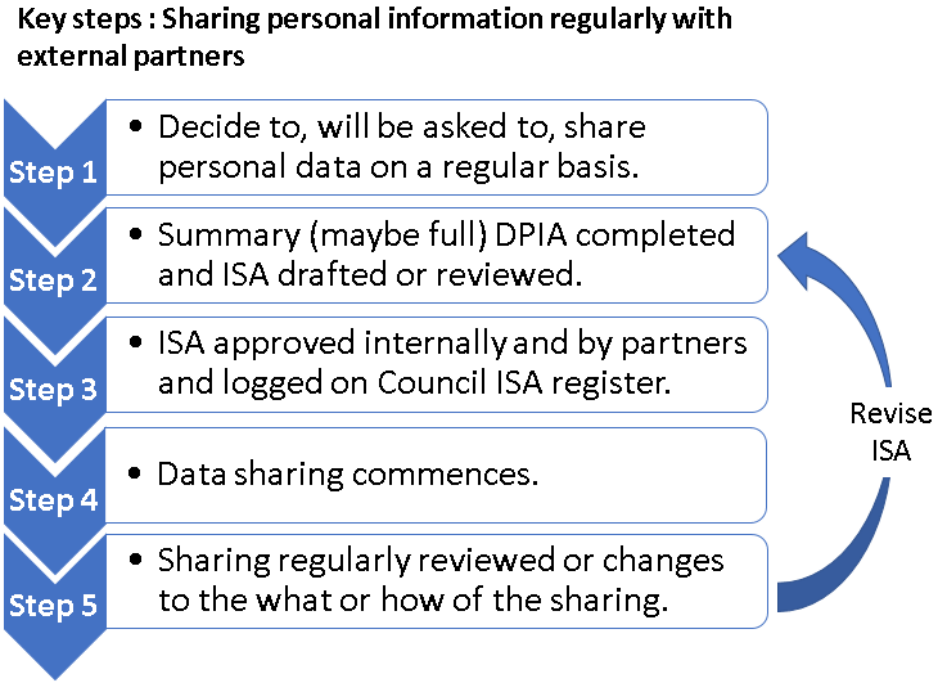
ISA Process Overview

32. There are two likely trigger mechanisms for the ISA procedure:

a) Where the Council wishes to initiate regular sharing of personal data with an external body.
b) Where the Council has received a request from an external body to share personal data on a regular basis.

33. An ISA flowchart (set out in Appendix A) will be hosted on the intranet as a guide for staff who wish to share information.

34. The process will typically follow the steps set out in the diagram below with the sections which follow providing more detail:



Council initiated information sharing

35. There are some practical and legal factors which should be considered when deciding whether to share data. Asking the following questions will help:

- What is the sharing meant to achieve? – there needs to be clear objectives
- What information needs to be shared to achieve the objectives?
- Is the sharing necessary and proportionate?
- Could the objectives be achieved without sharing the data or in a less intrusive way (e.g. anonymising the data)?
- What risks does the data sharing pose to individuals and are they likely to object?
- Can individuals be consulted about the sharing?
- Is it right to share data in this way?
- Will the data be shared securely?
- What would happen if we did not share the data?
- Who needs access to the shared data?
- When and how should we share it?
- How can we check the sharing is achieving its objectives?
- For how long is the sharing going to be required?

36. When wishing to share personal data on a regular basis with an external body, the Information Asset Manager (or their nominee) must complete a Summary DPIA and send it to the IG Team. The IG Team will assess whether a full DPIA will be required to identify risks and underpin the ISA. Where necessary the IG Team will seek more information on the proposed data sharing.

37. The Information Asset Manager (or their nominee) will be guided through the ISA process by the Information Governance Team who will call upon Legal Services where necessary.

38. The Council's ISA template will be used as the basis for all agreements initiated by the Council. The template will be maintained by Legal Services.

39. The Information Asset Manager (or their nominee) will ensure that there is a named single point of contact (SPoC) for the ISA. The SPoC will be named in the ISA.

40. The ISA will be informed by privacy risks (and mitigations) identified in the summary and / or full DPIA.

41. The DPO (or their nominee) will be consulted during the drafting of an ISA and associated DPIA in order to provide advice. The DPO will provide advice on the DPIA and ISA prior to sign-off.

Third party initiated information sharing

42. When a third party initiated ISA is received, the relevant Information Asset Owner or Manager (or their nominee) will send it to the IG Team for comment.

43. A summary, and occasionally a full, DPIA may be required to identify risks and their mitigations to underpin the assessment of whether the ISA should be signed.

44. The authoriser / signatory of the ISA (see next section) will take account of advice of the DPO (or the IG Team acting as the DPO's nominee) in deciding whether to agree to the ISA arrangements.

45. Until an ISA is signed-off relevant data should not be shared.

Authorisation and sign-off of ISAs

46. Arrangements for authorising the sign-off of all ISAs (and any subsequent amendments to the ISA) will be as follows:

    a) Where sharing relates to children or adults' health and/or care data, the relevant Information Asset Manager will authorise the sign-off of the ISA, seeking agreement from the Caldicott Guardian if considered necessary.
    b) Where information sharing is confined to the personal data of a particular directorate, the Information Asset Manager will authorise the sign-off of the ISA, seeking agreement from the Information Asset Owner if considered necessary. Information Asset Owner will authorise the sign-off.

47. Where the DPO (or their nominee) has significant concerns regarding the residual risks associated with the proposed sharing (i.e. risks which cannot be satisfactorily mitigated), they should refer the matter to the Senior Information Risk Owner (SIRO).

48. Appreciating that the authorisers / signatories of ISAs will be guided by IG advice, the DPO, IG Team and / or Legal Services may use the overview form at Appendix B to advise the authoriser / signatory of key issues associated with sharing and the associated ISA.

49. The sharing proposal / ISA (and associated DPIA) authorisation process may result in one of the following outcomes:

    - Authorise ISA as drafted
    - Authorise it with conditions such as risk mitigations to be put in place etc.
    - Defer it pending further refinement / risk mitigation
    - Reject it with no scope for refinement

50. In accordance with data protection law, the DPO must consult the Information Commissioner's Office on any data processing (including sharing) which gives rise to high risks to data subjects which cannot / will not be mitigated to an acceptable level. The DPO will consult with the SIRO prior to doing this.

51. Where the Council initiates an ISA and it progresses through the key steps of this procedure to sign-off, the Information Asset Manager (or their nominee) will

be responsible for ensuring that the ISA is signed off by all the sharing partners. They will also be responsible for ensuring any risk mitigations cited in the DPIA are carried out by the required due date.

52. Until an ISA is signed-off relevant data should not be shared.

Following approval (sign off) of an ISA

53. When finalised the ISA, whether initiated by the Council or a third party, will be sent to the IG Team by the Information Manager (or their nominee) for inclusion on the corporate ISA register.

54. Numbers of ISAs in progress or completed and any known risks / issues will be reported to the Information Governance and Cyber Security Board on a quarterly basis, or more frequently if required. This will require Information Asset Owners / Managers (or their nominees) and other parties to make the Information Governance Team aware of ISAs that are in progress / signed-off, in line with the provisions in this Procedure.

ISA amendment and review

55. ISA arrangement and associated DPIA should be reviewed on a regular basis because changes in circumstances or the rationale for the data sharing may arise at any point which may create new risk. The following questions should be asked regularly and no less than every two years:

- Is the data still needed and can it be justified?
- Are arrangements for informing people of the data sharing still adequate (e.g. are references to it in privacy notices still accurate)?
- Are your procedures for ensuring you comply with the requirements of the ISA still working in practice?
- Are you responding to queries and complaints effectively and analysing them to make improvements to data sharing arrangements?

56. The Single Point of Contact will typically be responsible for reviewing the ISA but the Information Asset Manager (or their nominee) may assign an appropriate staff member to undertake this task.

57. If there is a material change in the way the sharing operates, such as the introduction of new technology, or a widening of scope, the Information Asset Manager (or their nominee) or ISA Single Point of Contact should liaise with the Information Governance Team who will advise whether the change will require a new DPIA or review to an existing one prior to any revision of the ISA.

58. ISAs should be in place for no longer than six years. Any extension to this should prompt a new ISA and sign-off by partners.

Roles and Responsibilities

59. All staff including employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information staff must be aware of and comply with this procedure.

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

61. The Council's Data Protection Officer and Information Governance Team will ensure that the requirements described in this procedure are implemented and maintained.

Compliance with this Procedure

62. The Council wishes to foster a culture in which the benefits of appropriate and proportionate data sharing can be realised.

63. 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.

64. Unauthorised data sharing, which is the result of an intentional action or inaction, may constitute a personal data breach which may give rise to criminal charges under the Data Protection Act and Computer Misuse Act.

Review of this procedure

65. This procedure will be regularly monitored and reviewed by the Data Protection Officer (or their nominee) who will revise it in line with learning arising from the implementation of the procedure.

66. 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

67. If you have any issues over the clarity of this procedure, how it should be applied in practice or have any suggestions for amendments, please contact:

The Information Governance Team
Email: data.protection@nottscc.gov.uk
Telephone: 0115 8043800

68. Further reading and supporting information:

Title (as hypertext link) and publication date	Author
Data Sharing Code of Practice (September 2021)	ICO
Information sharing - Advice for practitioners providing safeguarding services to children, young people, parents and carers (July 2018)	HM Govt

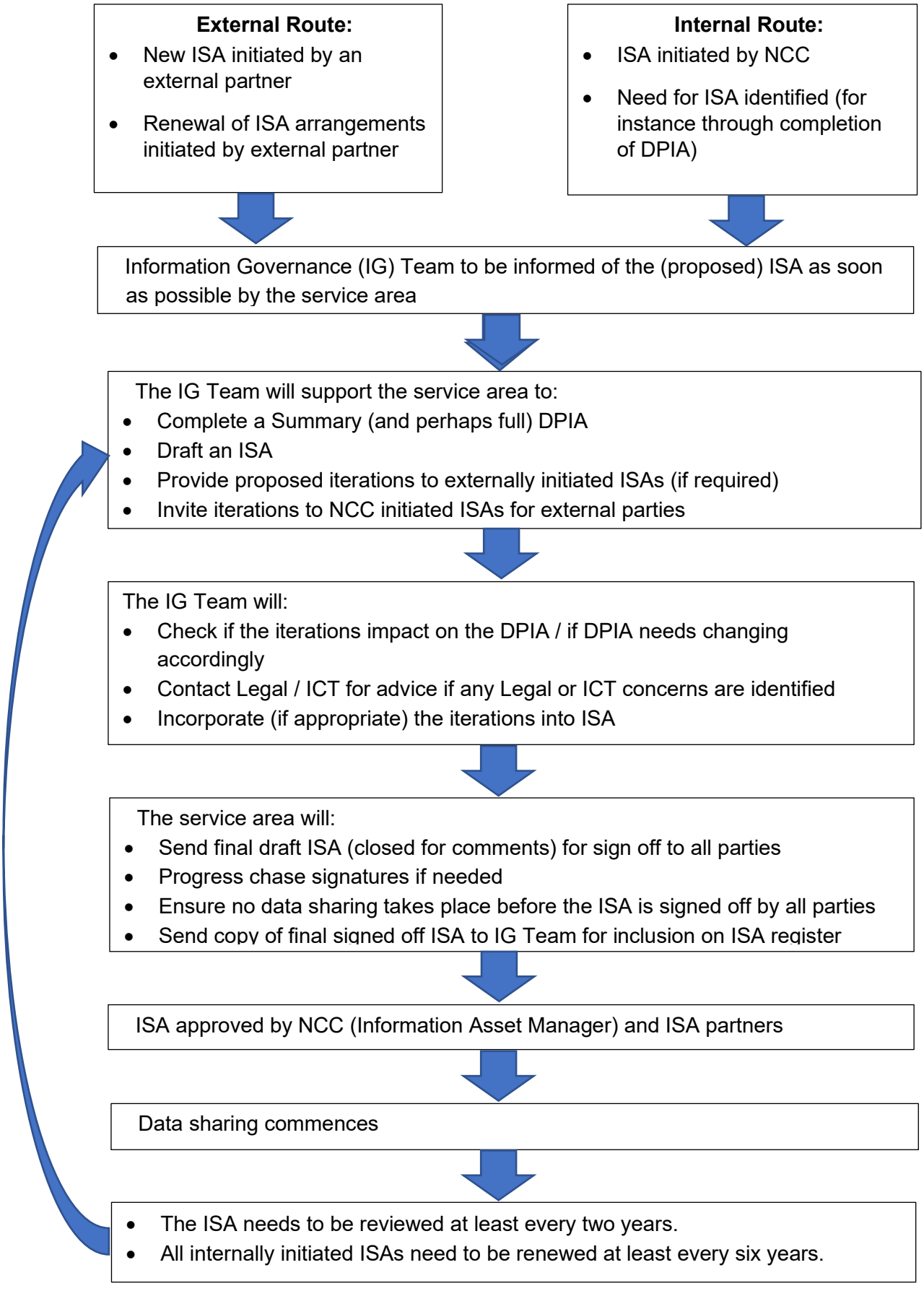
Document Control

Owner	Data Protection Officer
Author	Caroline Agnew, Data Protection Officer
Last Reviewer	Brendan Jennings, Information Governance Advisor
Approver	Jason Monks, Senior Information Governance Advisor (acting DPO)
Date of Approval	08 August 2022
Date of next review	08 August 2024
Version	2.1
Classification	Public

Version	Date	Changes and Approver
1.0	15/2/2018	Original document approved by Information Governance Group. It was authored by Simon Gill, Solicitor, Legal Services
2.0	11/12/2019	Major redraft. Changes to reflect ICO Data Sharing Code of Practice; add at a glance, advice and document control sections in line with other IG procedures; overall strengthening to give greater clarity on process and responsibilities including a deciding to share and review section; revised ISA signoff arrangements agreed by IGB
2.1		Minor amendments as part of regular review. No substantial changes to process.

Appendix A

Information Sharing Agreement Flowchart



Nottinghamshire County Council

Information Sharing Agreement Authoriser Assurance Form

To be used by the Info Gov. Team to provide assurance about, the proposed ISA to the NCC authoriser (e.g. SIRO / Caldicott Guardian). It should enable the authoriser to be able to take an informed decision based on the key facts given without reading all the ISA documents.

Deadline for sign-off			
ISA Start	Click here to enter a date.	ISA End	Click here to enter a date.

Name of ISA			
Is this an NCC initiated ISA?		**Yes** ☐	**No** ☐
NCC Team / ISA Lead Officer or SPOC			
Is this ISA initiated by a third party?		**Yes** ☐	**No** ☐
Name of initiating party (if not NCC)			

What will the sharing involve?	
Who are the parties to the ISA?	
What requirements are placed on NCC in the ISA and have these been addressed?	
Any risks / concerns identified?	
Any NCC DPO / Legal advice sought?	

IGT Recommendation for Signatory			
Approve ISA as drafted	☐	Defer & seek amendments	☐
Reject ISA as drafted	☐	Other	☐
Comments / advice:			
Name		**Date**	Click here to enter a date.
Title		**Email**	

Signatory Decision			
ISA to be signed as drafted	☐	Defer & seek amendments to ISA	☐
ISA to be rejected as drafted	☐	Other	☐

Comments:			
Name		**Date**	Click here to enter a date.
Title		**Email**	