NPCC Information Asset Ownership Policy

Version Record

Version No	Amendments Made	Authorisation
0.1	Initial draft by TLT Solicitors	Chief of Staff to the Chair of NPCC 23rd October 2020
1.0	Revised version	NPCC Command Team 5th December 2022

1 Introduction

1.1 The National Police Chiefs' Council (referred to in this Policy as the **NPCC, we, us** or **our**) has established this Policy to set out how **Information Asset Ownership** applies to the NPCC functions.

1.2 Information Asset Ownership was introduced across Her Majesty's Government (HMG), policing and the wider public sector following the 2008 Data Handling Review (DHR) as means of improving the security and use of information.

1.3 This policy sets out what NPCC Information Assets are, who the NPCC's Information Asset Owners (IAOs) are, and what is expected of them.

1.4 IAOs report to the **NPCC Senior Information Risk Owner (SIRO)** on matters pertaining to NPCC Information Asset Ownership. The NPCC SIRO for NPCC Information Assets is the Chair of the NPCC.

1.5 This policy applies to police officers, staff members and contractors who work within NPCC Strategic Hub, NPoCC and the NPCC Programmes[1], or are based at NPCC's London HQ (referred to in the remainder of this Code as **staff, staff member** or **you**).

1.6 This Policy does not apply to Information Assets in National Units or within National Databases/Systems.

1.7 The Information Assets created in connection with the functions of the NPCC Audit & Assurance Board (ABB) fall under the Information Asset Ownership of the Chair of the AAB. Copies of that material held by the NPCC fall under the Information Asset Ownership of Head of the Strategic Hub.

2 NPCC Information Assets

2.1 Information Assets**,** as per the HMG definition, are: "*bodies of information, defined and managed as a single unit so that they can be understood, shared, protected and exploited effectively. Information Assets have recognisable and manageable value, risk, content and lifecycles."*

2.2 **NPCC Information Assets** are Information Assets used in any way for the delivery of the functions of the NPCC. Those functions are set out within the NPCC Section 22A Collaboration Agreement.

2.3 NPCC Information Assets may be sub-divided for convenience into Sub-Assets.

[1] These include Inclusion & Race, Violence Against Women & Girls and Office of the Chief Scientific Officer

2.4 Information Assets used exclusively by the forces whose Chief Officers form the NPCC fall outside the scope of this Policy.

2.5 Some NPCC Information Assets may contain personal data and therefore are subject to the requirements of Data Protection legislation (Data Protection Act 2018 and UK GDPR).

2.6 NPCC Information Assets may be held digitally within the NPCC's or home force IT infrastructure, including the SharePoint, email, applications and databases. They can also exist in hard copy, in forms, in correspondence, in photographs or other images, as sound recordings, and in other documents.

3 Purpose of the Information Asset Owner

3.1 HMG guidance states:

"Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process."

3.2 An NPCC IAO is permitted to nominate officers or staff to undertake work on their behalf to best ensure the NPCC IAO's tasks are fulfilled (see section 5 for tasks). These individuals are termed **Information Asset Assistants (IAAs).** Even when work has been delegated in this manner the NPCC IAO retains responsibility and accountability for the NPCC Information Asset to which they have been designated as NPCC IAO.

4 Designation of NPCC Information Asset Owners

4.1 The NPCC's approach to Information Asset Ownership is to align it as closely as possible to existing business/operational structures and arrangements.

4.2 The table at Appendix A sets out the posts within NPCC designated by this Policy to act as NPCC IAOs, or IAAs.

5 Responsibilities and Tasks of NPCC Information Asset Owners

5.1 The table at Appendix B provides the IAO Responsibilities as set out in HMG guidance (grey boxes), together with the tasks identified by this Policy that NPCC IAOs are required to undertake arising from those responsibilities.

5.2 Information Asset Risks

5.3 Appendix C sets out potential information risks and an assessment template that may assist NPCC IAOs when conducting information risk assessments on their NPCC Information Assets.

5.4 By default, the NPCC adopts the police service's National Information Risk Appetite as determined by the Chair of NPCC Digital, Data and Technology Coordination Committee (formerly 'IMORCC') in their role as National Senior Information Risk Owner.

6 Annual Report to NPCC SIRO

6.1 On an annual basis each NPCC Information Asset Owner is required to provide a report to the NPCC SIRO. The template at Appendix D may be used for this purpose and assistance in completing it may be obtained from the NPCC Data Protection Officer (DPO). NPCC Information Asset Owners may wish to arrange for the production of separate reports for some or all of any Sub-Assets.

7 Records of Information Assets

7.1 Records of NPCC Information Assets are maintained within NPCC's Records of Processing Activities (RoPA) spreadsheet in the possession of the NPCC DPO. Within that document some NPCC Information Assets are sub-divided into Sub-Assets.

8 NPCC SIRO

8.1 The NPCC SIRO is permitted to nominate officers or staff, such as Strategic Risk & Planning Manager, to undertake work on their behalf to best ensure the NPCC SIRO's tasks are fulfilled.

Even when work has been delegated in this manner the NPCC SIRO retains responsibility and accountability.

9 Unclear Information Asset Ownership

9.1 Where it is unclear who the NPCC IAO is for a particular Information Asset, the Strategic Hub Lead is empowered to make that determination and may assume the IAO role themselves where they deem it appropriate.

10 Police Digital Service (PDS) SIRO

10.1 The PDS SIRO owns information risks relating to the PDS IT infrastructure on which most NPCC business is conducted. Consequently, NPCC IAOs are expected to engage with PDS when dealing with risks that may be associated with vulnerabilities to the PDS/NPCC IT infrastructure.

11 Training

11.1 The primary training material for NPCC IAOs is the 2018 IAO Handbook authorised by the Police Information Assurance Board (see Appendix E). Although designed for Police forces the handbook provides useful content applicable to the NPCC. Relevant tasks and responsibilities have been extracted from the handbook and included in this Policy.

11.2 The primary training material for the NPCC SIRO is the 2018 SIRO Handbook authorised by the Police Information Assurance Board (see Appendix F). SIRO training is available from the College of Policing.

11.3 Additional training or assistance for NPCC IAOs may be sourced from home force Information Security Officers and Data Protection Officers, or the NPCC Data Protection Officer.

Appendix A: NPCC Information Asset Owners

NPCC Information Asset Owner (Post)	**Information Asset Assistant (Post)** where designated by this Policy	**Information Asset Description** Note: for convenience these assets may be broken down locally into sub-assets
Head of Strategic Hub	Head of Business Support	Records created or obtained as required for Business Support functions
	Head of Communications	Records created or obtained as required for Communications functions
	Head of Organisational Development & Change Team	Records created or obtained as required for the organisational development and change model functions
	Head of Strategy, Planning & Performance Team	Records created or obtained as required for Strategy, Planning & Performance functions
	Audit & Assurance Board Secretariat	NPCC-held copies of records created or obtained as required for the functions of the NPCC Audit & Assurance Board
	Staff Officer to NPCC Chair	Records created or obtained as required for the management of the office of the Chair of NPCC
Chairs of NPCC Coordination Committees	NPCC Coordination Committee Coordinators	Records relating to the management of each NPCC Coordination Committee
	NPCC Portfolio & Working Group Leads	Records created or obtained as required for each Portfolio & Working Group respectively
Head of NPoCC		Records created or obtained as required for the delivery of NPoCC's functions
NPCC Programme Leads		Records created or obtained as required for the delivery of NPCC Programmes including Inclusion & Race, Violence Against Women & Girls and Office of the Chief Scientific Officer
Data Protection Officer (DPO)		Records created or obtained as required by the performance of the DPO role including Rights Applications
Freedom of Information (FOI) Officer		Records created or obtained as required to manage and respond to FOI Requests to the NPCC

Appendix B: Responsibilities and Tasks of NPCC Information Asset Owners

The table below sets out the IAO Responsibilities as documented in HMG guidance (grey boxes), together with the tasks that NPCC IAOs are required to undertake under this Policy arising from those responsibilities.

A. Lead and foster a culture that values, protects and uses information for the public good	
1	Undertake information management training at least annually
2	Contribute via Senior Leadership Team discussions and other means to the NPCC's plans to achieve and monitor the right culture regarding NPCC Information, and take visible steps to support and participate in those plans
3	Ensure compliance with the provisions of Data Protection legislations in respect of their NPCC Information Asset which includes personal data, in accordance with NPCC's compliance mechanisms and policies, liaising with the NPCC DPO as is necessary. This includes taking steps to ensure necessary data quality of personal data, appropriate security around personal data, and ensuring personal data is not retained longer than is necessary.
B. Know what information the asset holds, and what transfers into or out of it and why	
4	Maintain an understanding of their NPCC Information Asset and how it is used within their business area and across NPCC
5	Know to what extent their NPCC Information Asset contains Personal Data
6	Approve any sharing of their NPCC Information Asset beyond the NPCC and ensure necessary Data Sharing Agreements are in place and readily accessible
7	Implement an appropriate regime for the physical protection of information, whether in digital or physical format; using methods such as secure storage of information, clear-desk policies 'need-to-know' access and policy around remote working
8	Determine the retention period for their NPCC Information Asset and ensure its secure disposal when no longer required in accordance with the NPCC Review, Retention & Disposal Policy.
C. Know who has access and why, ensuring their use is monitored	
9	Document and an ensure the application of an access policy to their NPCC Information Asset
10	Regularly review access permissions or logs to ensure access is consistent with their access policy
D. Understand and address risks to the asset and provide assurance to the SIRO	
11	Regularly undertake information risk management for their NPCC Information Asset. Appendix C provides potential risks for consideration
12	Participate in the management of Data Breaches involving their NPCC Information Asset and adopt any learning gained
13	Provide an annual report to the NPCC SIRO on information risk management for their NPCC Information Asset (See Appendix D) using assistance of the DPO and Strategic Risk & Planning Manager as is necessary
E. Ensure the asset is fully used for the public good, including responding to access requests	
14	Identify and develop opportunities to exploit the use of their NPCC Information Asset for the public good

15	Ensure that appropriate assistance is provided to the NPFDU Data Protection Advisor and NPCC FOI Officer regarding any Right of Access or Freedom of Information application to their NPCC Information Asset to best ensure they are responded to within the statutory timescales

Appendix C: Generic Information Risks and Assessment Template

The table starting overleaf sets out potential information risks and assessment criteria that may assist NPCC IAOs when conducting information risk assessments on their NPCC Information Assets.

Column 1 contains generic information risks that could apply to the information asset.

Columns 2 and 3 should be used to record the results of a risk assessment that should be carried out on each potential risk, the numerical result of which should then be added to Column 4.

Once the risk assessment has been conducted the Information Asset Owner should determine against their risk appetite whether the risk should lead to termination of the use of the Information Asset, or alternatively can be tolerated, or transferred or treated. These terms are described below:

- Terminate – On rare occasions some risks are so far beyond the tolerance identified by the risk appetite or are assessed as having such a severe impact on the business that the Information Asset should not be held or used
- Tolerate – some risks are of a sufficiently low level that no actions need to be taken
- Transfer – on rare occasions it could be possible to transfer the risk to third-parties
- Treat – many risks can be treated or mitigated to reduce them to a level that is acceptable to the Information Asset Owner

Where the decision is to treat the risk the treatment to be applied should be added to Column 6.

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	5. Decision (Terminate, Tolerate, Transfer or Treat)	6. Risk Treatment to be adopted, and/or comments regarding the scoring
Confidentiality-related					
IR1. The Information Asset is accessible by people who should not have access to it	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR2. The Information Asset is on a system which is hosted/held on an insecure infrastructure or premises.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR3. People who should have access to the Information Asset have inappropriate levels of access to it	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR4. The Information Asset is accidentally disclosed inappropriately	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR5. The Information Asset is deliberately accessed or disclosed inappropriately	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR6. The Information Asset is held or used in an insecure environment	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR7. The Information Asset can be damaged or inappropriately deleted	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
Integrity-related	Likelihood	Severity	Overall Risk	Decision	Risk Treatment to be adopted/Comments
IR8. The integrity of the Information Asset is jeopardised i.e. it can be damaged/altered	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
Availability-related	Likelihood	Severity	Overall Risk	Decision	Risk Treatment to be adopted/Comments
IR9. The Information Asset is inaccessible to those who should have access to it	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR10. The Information Asset is not shared when it could/should be	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR11. The Information Asset is not exploited when it could be	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR12. The Information Asset cannot be found (e.g. physical documents or searching of IT)	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.

Legality-related	Likelihood	Severity	Overall Risk	Decision	Risk Treatment to be adopted/Comments
IR13. The purpose(s) of holding or using the Information Asset is unclear	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR14. For Personal Data - there is no lawful basis to hold or use the Information Asset	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR15. For Personal Data the Information Asset is being used unfairly or without transparency to data subjects	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR16. For Personal Data the Information Asset is being used for a purpose incompatible with the reason it was first used/collected	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR17. Pseudonymised versions of the Information Asset can be altered to identify individuals	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
Data Quality-related	Likelihood	Severity	Overall Risk	Decision	Risk Treatment to be adopted/Comments
IR18. The Information Asset is inaccurate	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR19. The Information Asset is incomplete	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR20. The Information Asset cannot be amended/corrected when it needs to be	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR21. Duplicate versions of the Information Asset exist	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
Records Management-related	Likelihood	Severity	Overall Risk	Decision	Risk Treatment to be adopted/Comments
IR22. Excessive information is held	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR23. The Information Asset is held longer than is necessary	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
IR24. The Information Asset cannot be deleted/disposed of when no longer required	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
Training-related	Likelihood	Severity	Overall Risk	Decision	Risk Treatment to be adopted/Comments
IR25. Users of the Information Asset are inadequately trained	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Overtype here.
Governance-related	Likelihood	Severity	Overall Risk	Decision	Risk Treatment to be adopted/Comments

IR26. There is inadequate policy or procedure surrounding the access or use of the Information Asset	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Overtype here.**
IR27. There is an absence of an adequate information sharing agreement (where one is required) for the Information Asset	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Overtype here.**
IR28. There is an absence of a Data Processing Contract (where one is required) for the Information Asset	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Overtype here.**
IR29. Generally, there is inadequate governance for the Information Asset	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Overtype here.**
Ethical-related	Likelihood	Severity	Overall Risk	Decision	Risk Treatment to be adopted/Comments
IR30. The Information Asset is inappropriately discriminatory	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Overtype here.**
IR31. For Personal Data - Data Subjects are unaware of their rights regarding the Information Asset	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Overtype here.**
Miscellaneous	Likelihood	Severity	Overall Risk	Decision	Risk Treatment to be adopted/Comments
IR32. Click or tap here to add any risk not included above.	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Overtype here.**
IR33. Click or tap here to add any risk not included above.	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Overtype here.**
IR34. Click or tap here to add any risk not included above.	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Overtype here.**
IR35. Click or tap here to add any risk not included above.	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Overtype here.**

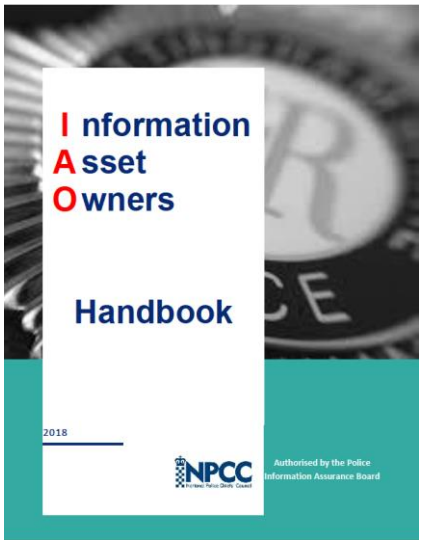
.

Appendix D: Annual Report to NPCC SIRO Template

Information Asset:	
Information Asset Owner:	
Date Completed:	

	NPCC Information Asset Owner Task	**NPCC Information Asset Owner's Evidence in Response to Task**
1	Undertake information management training at least annually	
2	Contribute to the NPCC's plans to achieve and monitor the right culture regarding NPCC Information, and take visible steps to support and participate in those plans	
3	Ensure compliance with the provisions of Data Protection legislations in respect of their NPCC Information Asset which is personal data, in accordance with NPCC's compliance mechanisms and policies, liaising with the NPCC DPO as is necessary	
4	Maintain an understanding of their NPCC Information Asset and how it is used within their business area and across NPCC	
5	Know to what extent their NPCC Information Asset contains Personal Data	
6	Approve any sharing of their NPCC Information Asset beyond the NPCC and ensure necessary Data Sharing Agreements are in place and readily accessible	
7	Implement an appropriate regime for the physical protection of personal information, whether in digital or physical format	
8	Determine the retention period for their NPCC Information Asset and ensure its secure disposal when no longer required	
9	Document and an ensure the application of an access policy to their NPCC Information Asset	
10	Regularly review access permissions or logs to ensure access is consistent with their access policy	
11	Regularly undertake information risk management for their NPCC Information Asset. Appendix C provides potential risks for consideration and an assessment template	
12	Participate in the management of Data Breaches involving their NPCC Information Asset and adopt any learning gained	
13	Provide an annual report to the NPCC SIRO on information risk management for their NPCC Information Asset (See Appendix D)	This document
14	Identify and develop opportunities to exploit the use of their NPCC Information Asset for the public good	
15	Ensure that appropriate assistance is provided to the NPFDU Data Protection Advisor and NPCC FOI Officer regarding any Right of Access or Freedom of Information application to their NPCC Information Asset to best ensure they are responded to within the statutory timescales	

Appendix E: NPCC IAO Handbook



Appendix F: NPCC SIRO Handbook