Data Protection Impact Assessment: IOM Scheme

Version: V0.1
Date: November 2018
Author: Insp Danny Kett
Owner:

Document Control

Sign-Off Details			
Sign-Off Authorities	**Role**	**Date**	**Signature**

Distribution List			
Name	**Role**	**Version**	**Date**

Version Control		
Version	**Date**	**Summary of Changes**
V0.1	Nov 2018	Initial input

Contents

List of Annexes –

1. Executive Summary

1.1.

1.2.

1.3.

1.4.

1.5.

2. Purpose of a DPIA

2.1. The Data Protection Impact Assessment (DPIA) is a flexible process which assists organisations in identifying and minimising the privacy risks of new projects or policies. Conducting a DPIA involves working with people within the organisation, with partner organisations and with the people affected to identify and reduce privacy risks. A DPIA will help to ensure potential problems are identified at an early stage and benefit organisations by producing better policies and systems and improving the relationship between organisations and individuals.

2.2. A Data Protection Impact Assessment will aim to incorporate the following process:

- Identify the need for a DPIA
- Describe the processing;
- Consultation process;
- Assess necessity and proportionality;
- Identify and assess risks;
- Identify measures to reduce risk;
- Sign-off and record the DPIA outcomes
- Integrate the DPIA outcomes into the project plan.

2.3. The Accountability and Governance: Data Protection Impact Assessments (DPIAs) guidance released by the Information Commissioner's Office (ICO) in March 2018 has been used to support this DPIA.

3. Structure of this Document

This document explains:

- What is Integrated Offender Management?
- What are the aims and benefits?
- How the steps from the Information Commissioners Data Protection Impact Assessments guidance been addressed, including:

  Step 1 – Identify the need for a Data Protection Impact Assessment (DPIA)
  Step 2 – Describe the processing
  Step 3 – Consultation process
  Step 4 – Assess necessity and proportionality
  Step 5 – Identify and assess risks
  Step 6 – Identify measures to reduce risk
  Step 7 – Sign off and record outcomes

Documentation supporting the DPIA is contained as Annexes, including:

Annex A: DPIA Screening Checklist
Annex B: Examples of High Risk Processing

What is Integrated Offender Management?

3.1. The Integrated Offender Management (IOM) scheme is a partnership with a vision to 'reduce the reoffending by those causing the most harm to communities within Norfolk and Suffolk'

3.2. The IOM was formed by the Norfolk and Suffolk Criminal Justice Board under the IOM Governance Board, to provide an interagency response to manage prolific and chaotic offenders within the counties.

3.3. The IOM adheres to the six key principles of IOM as laid down by the Home Office and the Ministry of Justice (2015).

3.4. **Aims**:

- All partners managing offenders together
- To deliver a local response to local problems
- With all offenders potentially in scope
- Facing up to their responsibility or facing the consequences
- With best use made of existing programmes and governance arrangements
- To achieve long-term desistance from crime.

3.5. **Benefits:**

Partnership working and supported business planning, services are commissioned and which prioritise structured interventions to reduce the risk of harm to communities, through rehabilitative practices and where necessary a swift return to the courts.

4. Step 1 - Identify the Need for a DPIA

4.1. In accordance with the ICO guidance, a screening checklist will need to be completed to determine if a DPIA is necessary, please find the checklist at Annex A.

4.2. If after completing the screening checklist, you are required to complete a DPIA, please answer the following questions. You may find it helpful to refer or link to other documents, such as a project proposal.

4.3. **Explain broadly what the project aims to achieve.**

The IOM Scheme aims to achieve the reduction of offending by the county's prolific, priority offenders.

4.4. **What type of processing does the project involve?**

The Scheme involves the process of personal, special category and criminal conviction and offence data. It involves an adoption assessment of cohort members, continuous monitoring of criminogenic needs and the assessment of outcomes at the point of de-registrations.

4.5. **Summarise why you identified the need for a DPIA.**

The overall outcome of completing this DPIA is to give an overview of the project and any compliance concerns. The IOM Scheme has been identified as requiring a DPIA due to the level of risk regarding the information that is being managed. It involves combining, comparing and matching data from multiple sources, evaluation and scoring, and the processing of sensitive data.

5. Step 2 – Describe the Processing

5.1. As part of the DPIA process, organisations should describe how information is collected, stored, used, retained and deleted.

5.2. **Describe the nature of processing:**

5.3. **How is information collected?**

Information is collated from conviction history, lifestyle information from the service user, probation and CRC records, Offender Group Reconviction Scale outcomes and relevant intelligence. This is used to identify an offenders' suitability for adoption on to the IOM scheme.

The collection of data is the start of the information management process. It affects all other stages of information management, from how the information is recorded to how long it will be retained. It is essential that information is collected, recorded and evaluated in a consistent manner across organisational and force boundaries. The College of Policing has published the Information Management Authorised Professional Practice (APP) to assist forces with their data collection and recording responsibilities, which can be found at: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/collection-and-recording/

5.4. **How is information used?**

To assess the service-users: suitability for adoption, progress through the scheme and de-registration outcomes.

5.5. **How is information stored?**

It is stored electronically within the Schemes' ECINS multiagency case management software and the IOM performance management tool.

5.6. **How is information reviewed, retained and deleted?**

The information collected is subject to the Management of Police Information Guidance (MoPI). There have been conversations with the administrators of ECINS to ensure that the weeding facility is possible. Currently there is no IOM data that meets the retention criteria for weeding as yet.

5.7. **What is the source of the data?**

Police National Computer Records, Probation Services Records, Prison information

5.8. **Will you be sharing the data with anyone?**

Partnerships within the scheme subject to the Information Sharing Agreement

Where data is used for research purposes this will be overseen by the scheme manager and any person with access to the data will comply with the relevant levels of vetting.

5.9. **What types of processing identified as likely high risk are involved?**

From the DPIA checklist it was identified that the IOM Scheme combines, compares and matches sensitive data from multiple sources. It was also identified that the individuals subject to the scheme are evaluated and scored.

5.10. **Describe the scope of the processing:**

5.11. **What is the nature of the data? Does it include special category or criminal offence data?**

The nature of the data included in the Scheme is a combination of all personal data, special category data and criminal conviction and offence data. Criminal offence data is a central tenant of the work undertaken within IOM.

5.12. **How much data will you be collecting and using?**

This will involve a large quantity of data pertaining to the life and activities of those registered for the IOM scheme or referred for registration.

5.13. **How often will you be collecting and using data?**

The data will be collected and used on a daily basis.

5.14. **How long are you retaining the data?**

Six years from the data of an individual's deregistration, this is for civil litigation threshold purposes.

5.15. **How many individuals are affected by the processing?**

All individuals that are subject to the scheme or subject to referral are affected by the processing.

5.16. **What geographical area does it cover?**

Norfolk and Suffolk, information may be shared across boarder where there is a business need.

5.17. **Describe the context of the processing:**

5.18. **What is the nature of your relationship with the individuals?**

Individuals subject to data processing will be offenders within the community, both within their statutory supervision and post-supervision.

5.19. **How much control will the individuals have?**

Individuals have very little control over the processing. In some instances they have control over which partner agencies that they engage with, however it is likely that their referral to a partner agency has been subject to a probation order.

5.20. **Would the individuals expect you to use their data in this way?**

The use of this data for the purpose described should not be unexpected in the context of rehabilitation and risk management.

5.21. **Do they include children or other vulnerable groups?**

Yes. Information regarding the children and dependents of service users will be collected and monitored for safeguarding purposes. Some offenders are also deemed vulnerable due to their age, health, circumstances.

5.22. **Are there prior concerns over this type of processing or security flaws?**

Schemes like the IOM operate in several forces and there have been no concerns. Although there are a variety of organisations inputting the data into ECINS, it a well-established national system that is used regularly by those involved.

5.23. **Is the processing novel in any way?**

The overarching IOM is not new and takes place across many police forces. However, this is a newly developed process for managing IOM cohorts, which is receiving national attention and being replicated in other IOM areas.

5.24. **What is the current state of technology in this area?**

- ECINS used for case management
- In House Database for performance management

- BUDDI Eagle Platform for the electronic GPS monitoring of a limited number of service users.

5.25. **Are there any current issues of public concern that you should factor in?**

Cannot foresee and public concern over this processing. It is thought the Public would see the benefits of increased public safety and less reoffending.

5.26. **Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?**

There is no approved code of conduct or certification however; the scheme follows National Guidance from the Home Office and Ministry of Justice.

5.27. **Describe the purposes of the processing:**

5.28. **What do you want to achieve?**

We want to achieve the long term reduction in offending through rehabilitation, or the management of risk through swift criminal justice intervention.

5.29. **What is the intended effect on individuals?**

The intended effect on individuals is for them to progress to be law-abiding with pro-social behaviour and improved quality of life.

5.30. **What are the benefits of the processing for you, and more broadly?**

The benefits of the processing is efficient and effective, evidence based management of the IOM scheme. The Scheme benefits the police force as it aims to reduce recidivism.

6. Step 3 – Consultation Process

6.1. As part of the DPIA process, you must consider how to consult with relevant stakeholders.

6.2. **Describe when and how you will seek individuals' views – or justify why it is not appropriate to do so.**

As this processing was taking place before the implementation of the new Data Protection requirements, consultation will take place with internal stakeholders.

6.3. **Who else do you need to involve within the Constabulary?**

The views will be sought from core areas of the Information Management Department; Records Management, Information Security and Data Protection.

6.4. **Do you need to ask any processors to assist?**

Not applicable

6.5. **Do you plan to consult information security experts, or any other experts?**

As stated above, The Constabularies' Information Security team will be consulted.

7. Step 4 – Assess Necessity and Proportionality

7.1. This chapter details the compliance and proportionality measures that are in place for the processing.

7.2. **What is your lawful basis for processing?**

Data Protection Act 2018 Part 3 Chapter 1 Section 31 – The Law Enforcement purpose – the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

7.3. **Does the processing actually achieve your purpose?**

Yes, this is a holistic approach to integrated offender management.

7.4. **Is there any other way to achieve the same outcome?**

No, there is not another collaborated multi-agency scheme that allows the agencies to work together efficiently.

7.5. **How will you prevent function creep?**

The scheme operates within the auspices of an agreed operating model.

7.6. **How will you ensure data quality and data minimisation?**

Managers of the Scheme dip sample records and entries to ensure data quality and minimisation.

7.7. **What information will you give individuals?**
Individuals will be informed that they are subject to the IOM scheme. If required individuals can be provided with the Forces' Information Charter that outlines the Constabularies' processing activities.

7.8. **How will you support individuals' rights?**
The individuals' rights will be maintained throughout the process. All information held can be retrieved for the purpose of fulfilling individuals' rights under the Data Protection legislation.

7.9. **What measures do you take to ensure processors comply?**
The internal processes of the data have measures such as; access to records limited to those directly working within the IOM scheme, review of users bi-monthly by the scheme manager to ensure all users are actively involved in IOM scheme delivery.

7.10. **How do you safeguard any international transfers?**
There are no international transfers; the servers are all within the UK.

8. Step 5 – Identify and Assess risks

8.1. This chapter details the privacy issues, identified with IOM, associated risks and an indication of the potential harm.

Privacy issue	Associated risks	Likelihood of harm	Severity of harm	Overall risk
Potential impact on individual.	Source of risk. Include associated compliance and corporate risks as necessary.	Remote / Possible / Probable	Minimal / Significant / Severe	Low / Medium / High
A. Obtaining				
Data subjects may feel their personal data is being obtained unfairly.	Non-compliance with the GDPR, DPA and HRA.	Remote	Significant	Medium
	Associated reputational damage to forces including financial and legal risks.	Remote	Significant	Medium
	Loss of public confidence.	Remote	Minimal	Low
	Reluctance to provide information to the police.	Remote	Minimal	Low
Data subjects may consider the amount of information being obtained is excessive.	Non-compliance with the GDPR, DPA and HRA.	Possible	Minimal	Low
	Associated reputational damage to forces including financial and legal risks.	Remote	Minimal	Low
	Loss of public confidence.	Remote	Minimal	Low
	Reluctance to provide information to the police.	Remote	Minimal	Low
B. Processing				
Data subjects may feel that access to their personal data is	Non-compliance with the GDPR, DPA and HRA.	Possible	Minimal	Low

made too widely available within the Athena forces. Data subjects may feel the processing is a disproportionate intrusion of their privacy.	Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	Possible Possible Possible	Minimal Minimal Minimal	Low Low Low
C. Disclosing				
Data subjects may have concerns regarding the disclosure of their personal data with the police service.	Non-compliance with the GDPR, DPA and HRA. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	Possible Possible Possible Possible	Minimal Minimal Minimal Minimal	Low Low Low Low
Data subjects many have concerns regarding the disclosure of their personal data to partner agencies. E.g. Community Safety Partnerships	Non-compliance with the GDPR, DPA and HRA. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	Possible Possible Possible Possible	Minimal Minimal Minimal Minimal	Low Low Low Low
Data subjects many have concerns regarding the disclosure of their personal data outside of the police service	Non-compliance with the GDPR, DPA and HRA. Associated reputational damage to	Possible	Minimal	Low

E.g. Home Office data hub, HMRC.	forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	Possible Possible Possible	Minimal Minimal Minimal	Low Low Low
D. Data Quality				
Data subjects may have concerns regarding the accuracy, reliability, adequacy of their data	Non-compliance with the GDPR, DPA and HRA. Associated risks to forces including decision making being compromised based on poor data quality, which could lead to operational harm, inefficiency, duplication of effort and failure to link related pieces of information. As a consequence, this could lead to associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	Possible Possible Remote Remote	Minimal Significant Minimal Minimal	Low Medium Low Low
IOM users may have concerns regarding the accuracy, reliability, adequacy of their data	Non-compliance with the GDPR, DPA and HRA. Associated risks to forces including decision making being compromised based on poor data quality, which could lead to operational harm, inefficiency, duplication of effort and failure to link related pieces of	Remote Possible	Minimal Significant	Low Medium

	information. As a consequence, this could lead to associated reputational damage to forces including financial and legal risks.			
	Loss of public confidence.	Remote	Minimal	Low
	Reluctance to provide information to the police.	Remote	Minimal	Low
	Loss of confidence by users of the systems.	Remote	Minimal	Low
	Searching of the system will be more time consuming and further lead to correction reports	Remote	Minimal	Low
E. Security				
Data subjects may have concerns regarding the security of their data	Failure to protect personal data can result in non-compliance with GDPR, DPA and/or HRA (Right to respect for private/family life).	Remote	Minimal	Low
	Operational matters could be compromised as a result of ineffective security, leading to harm to individuals, organisation, investigation, bringing offenders to justice.	Possible	Significant	Medium
	Associated reputational damage to forces including financial and legal risks.	Possible	Significant	Medium
	Loss of public confidence.	Remote	Minimal	Low
	Reluctance to provide information to the	Remote	Minimal	Low

	police.			
IOM users may have concerns regarding the security of the data	Failure to protect personal data can result in non-compliance with GDPR, DPA and/or HRA (Right to respect for private/family life). Operational matters could be compromised as a result of ineffective security, leading to harm to individuals, organisation, investigation, bringing offenders to justice. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police. Loss of confidence by users of the systems.	Remote Possible Possible Remote Remote Possible	Minimal Significant Significant Minimal Minimal Minimal	Low Medium Medium Low Low Medium
F. Review, Retention & Disposal				
Data subjects may have concerns regarding the length of time their personal data is being held and affecting their right to privacy.	Failure to protect personal data can result in non-compliance with GDPR, DPA and/or HRA (Right to respect for private/family life). Operational matters could be compromised as a result of	Possible Possible	Minimal Minimal	Low Low

	ineffective security, leading to harm to individuals, organisation, investigation, bringing offenders to justice. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	Possible Possible Possible	Minimal Minimal Minimal	Low Low Low
IOM users may have concerns that information is removed prematurely and prejudicing operational policing matters and Disclosure and Barring decisions.	Failure to protect personal data can result in non-compliance with GDPR, DPA and/or HRA (Right to respect for private/family life). Operational matters could be compromised as a result of premature weeding of information resulting in harm to individuals, organisation, investigations and bringing offenders to justice. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police. Loss of confidence by users of the systems.	Possible Possible Possible Possible Possible Possible	Remote Remote Remote Remote Remote Remote	Low Low Low Low Low Low
Data subjects may have concerns regarding the reviewing of their	Failure to protect review personal data can result in non-compliance with	Possible	Minimal	Low

personal data and whether the process is being undertaken appropriately.	GDPR, DPA, HRA (Right to respect for private/family life) and the College of Policing APP Information Management. Operational matters could be compromised as a result of ineffective reviewing of information, resulting in harm to individuals, organisation, investigations and bringing offenders to justice. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	Possible Possible Possible Possible	Minimal Minimal Minimal Minimal	Low Low Low Low
Data subjects may have concerns regarding the secure manner in which their personal data weeded.	Failure to protect review personal data can result in non-compliance with GDPR, DPA, HRA (Right to respect for private/family life) and the College of Policing APP Information Management. Operational matters could be compromised as a result of ineffective reviewing of information, resulting in harm to individuals, organisation, investigations and bringing offenders to justice. Associated reputational damage to forces including	Possible Possible Possible	Minimal Minimal Minimal	Low Low Low

	financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	 Possible Possible	 Minimal Minimal	 Low Low
G. Subject Rights				
Data subjects may have concerns regarding the application of their statutory information rights under the DPA and FOIA.	Failure to respond to applications in a timely and comprehensive manner - can result in non-compliance with GDPR, DPA, HRA (Right to respect for private/family life) and the College of Policing APP Information Management. Operational matters could be compromised as a result of ineffective reviewing of information, resulting in harm to individuals, organisation, investigations and bringing offenders to justice. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	Possible Possible Possible Possible Possible	Minimal Minimal Minimal Minimal Minimal	Low Low Low Low Low
IOM users may have concerns regarding the application of individual's applying their statutory rights under the GDPR and DPA – which may result in information being disclosed in	Operational matters could be compromised as a result of ineffective reviewing of information, resulting in harm to individuals, organisation, investigations and bringing offenders to	Possible	Significant	Medium

advance of thorough assessment of impact on operational matters.	justice. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police. Loss of confidence by users of the systems.	Possible Possible Possible Possible	Significant Significant Significant Significant	Medium Medium Medium Medium

9. Step 6 – Identify Measures to Reduce Risk

9.1. This chapter details the measures engaged to reduce or eliminate risks identified as medium or high risk in Step 5.

Privacy Issue	Associated Risks	Mitigation	Effect on Risk	Residual Risk	Measure Approved
Potential impact on individual.	Source of risk. Include associated compliance and corporate risks as necessary.	Options to reduce or eliminate risk	Eliminated / Reduced / Accepted	Low / Medium / High	Yes / No
A. Obtaining					
Data subjects may feel their personal data is being obtained unfairly.	Non-compliance with the GDPR, DPA and HRA. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	The Information used to facilitate the scheme is information that is obtained for the prevention and detection of crime. The second use of the information is still for a policing purpose. Subjects are aware they are on the scheme and can be provided with the Constabularies' Information Charter. The Information Management Business Area (IMBA) has a person of chief officer rank known as the Director of Information, who maintains a portfolio for data protection, freedom of information and records management. This role promotes compliance, consistency and a corporate approach across the police service. The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in their statutory responsibility to comply with the Data Protection Act, which can be found at: http://www.app.college.police.uk/app-content/information-management/data-protection/ Contained within the APP is guidance to forces on fair and lawful processing: http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-1-fair-and-lawful-processing	Reduced	Low	Yes

		This further includes guidance on the obtaining by the police of personal data: http://www.app.college.police.uk/app-content/information-management/data-protection/#fair-processing-requirements-obtaining **Note**: Under, a Fair Processing notice may not have to be provided where doing so would likely prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders. The collection of data is the start of the information management process. It affects all other stages of information management, from how the information is recorded to how long it will be retained. It is essential that information is collected, recorded and evaluated in a consistent manner across organisational and force boundaries. The College of Policing has published the Information Management Authorised Professional Practice (APP) to assist forces with their data collection and recording responsibilities, which can be found at: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/collection-and-recording/			
Data subjects may consider the amount of information being obtained is excessive.	Non-compliance with the GDPR, DPA and HRA. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the	The amount of data collected is from a range of agencies however, the information is required in order to facilitate the scheme. The Information Management Business Area (IMBA) has a person of chief officer rank known as the Director of Information, who maintains a portfolio for data protection, freedom of information and records management. This role promotes compliance, consistency and a corporate approach across the police service. The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in their statutory responsibility to comply with the Data Protection Act, which can be found at:	Accepted	Low	Yes

	police.	http://www.app.college.police.uk/app-content/information-management/data-protection/ Contained within the APP is guidance to forces on fair and lawful processing: http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-1-fair-and-lawful-processing This further includes guidance on the obtaining by the police of personal data: http://www.app.college.police.uk/app-content/information-management/data-protection/#fair-processing-requirements-obtaining **Note**: Under DPA, a fair processing notice may not have to be provided where doing so would likely prejudice preventing or detecting crime, or apprehending or prosecuting offenders. The collection of data is the start of the information management process. It affects all other stages of information management, from how the information is recorded to how long it will be retained. It is essential that information is collected, recorded and evaluated in a consistent manner across organisational and force boundaries. The College of Policing has published the Information Management Authorised Professional Practice (APP) to assist forces with their data collection and recording responsibilities, which can be found at: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/collection-and-recording/			
B. Processing					
Data subjects may feel that access to their personal data is made too widely available within	Non-compliance with the GDPR, DPA and HRA. Associated reputational damage to	Only staff working within the IOM scheme will have access to the information relating to the Scheme. The Information Management Business Area (IMBA) has a person of chief officer rank known as the Director of	Reduced	Low	Yes

the Athena forces. Data subjects may feel the processing is a disproportionate intrusion of their privacy.	forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	Information, who maintains a portfolio for data protection, freedom of information and records management. This role promotes compliance, consistency and a corporate approach across the police service. The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in their statutory responsibility to comply with the Data Protection Act, which can be found at: http://www.app.college.police.uk/app-content/information-management/data-protection/ Contained within the APP is guidance to forces on fair and lawful processing: http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-1-fair-and-lawful-processing This further includes guidance on the processing by the police of personal data: http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-1-fair-and-lawful-processing **Note**: Under DPA, a Fair Processing notice may not have to be provided where doing so would likely prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.			
C. Disclosing					
Data subjects may have concerns regarding the disclosure of their personal data with the police service.	Non-compliance with the GDPR, DPA and HRA. Associated reputational damage to forces including financial and legal risks. Loss of public	Data will not be shared outside the individuals that are responsible for delivering the Scheme unless there is an established operational need. The College of Policing has published the Information Management APP which can be found at: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/ This further includes guidance to forces on the sharing of police information, which can be found at: http://www.app.college.police.uk/app-content/information-	Reduced	Low	Yes

	confidence. Reluctance to provide information to the police.	management/management-of-police-information/sharing/			
Data subjects many have concerns regarding the disclosure of their personal data to partner agencies. E.g. Community Safety Partnerships	Non-compliance with the GDPR, DPA and HRA. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	There is an Information Sharing Agreement in place to facilitate the sharing between the partner agencies; this ensures compliance with the GDPR, DPA and appropriate safeguards. The College of Policing has published the Information Management APP which can be found at: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/ This further includes guidance to forces on the sharing of police information, which can be found at: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/sharing/	Reduced	Low	Yes
Data subjects many have concerns regarding the disclosure of their personal data outside of the police service E.g. Home Office data hub, HMRC.	Non-compliance with the GDPR, DPA and HRA. Associated reputational damage to forces including financial and legal risks.	There is an Information Sharing Agreement in place to facilitate the sharing between the partner agencies; this ensures compliance with the GDPR, DPA and appropriate safeguards. The College of Policing has published the Information Management APP which can be found at: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/ This further includes guidance to forces on the sharing of	Reduced	Low	Yes

	Loss of public confidence. Reluctance to provide information to the police.	police information, which can be found at: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/sharing/			
D. Data Quality					
Data subjects may have concerns regarding the accuracy, reliability, adequacy of their data	Non-compliance with the GDPR, DPA and HRA. Associated risks to forces including decision making being compromised based on poor data quality, which could lead to operational harm, inefficiency, duplication of effort and failure to link related pieces of information. As a consequence, this could lead to associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	The individuals that manage the Scheme dip sample the information to ensure the accuracy and reliability of the data. Data Subjects have their individual rights under the DPA to ensure inaccurate data is rectified or erased. The Information Management Business Area (IMBA) has a person of chief officer rank known as the Director of Information, who maintains a portfolio for data protection, freedom of information and records management. This role promotes compliance, consistency and a corporate approach across the police service. The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in their statutory responsibility to comply with the Data Protection Act, which can be found at: http://www.app.college.police.uk/app-content/information-management/data-protection/ Contained within the APP is guidance to forces on adequacy and relevancy issues: http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-three-adequate-relevant-and-not-excessive This further includes guidance on the accuracy of personal data: http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-four-accurate-and-up-to-date The College of Policing has published the Information Management APP within which is included guidance for	Reduced	Low	Yes

		forces on the Data Quality principles: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/collection-and-recording/#data-quality-principles Readers are also asked to refer to Section G of this table – Subject Rights (individuals have a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed).			
IOM users may have concerns regarding the accuracy, reliability, adequacy of their data	Non-compliance with the GDPR, DPA and HRA. Associated risks to forces including decision making being compromised based on poor data quality, which could lead to operational harm, inefficiency, duplication of effort and failure to link related pieces of information. As a consequence, this could lead to associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the	The IOM users are aware of the requirements relating to data accuracy and reliability. Users are aware of the required fields to be completed. The information is also dip sampled by the users to ensure accuracy. The Information Management Business Area (IMBA) has a person of chief officer rank known as the Director of Information, who maintains a portfolio for data protection, freedom of information and records management. This role promotes compliance, consistency and a corporate approach across the police service. The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in their statutory responsibility to comply with the Data Protection Act, which can be found at: http://www.app.college.police.uk/app-content/information-management/data-protection/ Contained within the APP is guidance to forces on adequacy and relevancy issues: http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-three-adequate-relevant-and-not-excessive This further includes guidance on the accuracy of personal data: http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-four-accurate-and-up-to-date	Reduced	Low	Yes

	police. Loss of confidence by users of the systems. Searching of the system will be more time consuming and further lead to correction reports.	The College of Policing has published the Information Management APP within which is included guidance for forces on the Data Quality principles: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/collection-and-recording/#data-quality-principles			
E. Security					

Data subjects may have concerns regarding the security of their data	Failure to protect personal data can result in non-compliance with GDPR, DPA and/or HRA (Right to respect for private/family life). Operational matters could be compromised as a result of ineffective security, leading to harm to individuals, organisation, investigation, bringing offenders to justice. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	Only individuals that should have a policing purpose are able to access the information. Sensitive operational information would not be shared on the partnership system. Where appropriate reference to an Athena record, custody record or CAD may be made to inform that further information exists The Information Management Business Area (IMBA) has a person of chief officer rank known as the Director of Information, who maintains a portfolio for data protection, freedom of information and records management. This role promotes compliance, consistency and a corporate approach across the police service. The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in their statutory responsibility to comply with the Data Protection Act, which can be found at: http://www.app.college.police.uk/app-content/information-management/data-protection/ Contained within the APP is guidance to forces on security issues: http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-seven-security-and-protective-measures Personnel Security Vetting is an important process for enhancing the integrity and security of the police community. The Association of Chief Police Officers (ACPO) and the Association of Chief Police Officers in Scotland (ACPOS) has published a National Vetting Policy for the Police Community to support that commitment:- http://www.acpo.police.uk/documents/workforce/2012/201205-wfdba-vetting-policy.pdf ACPO/ACPOS recognise that information, including the supporting processes, systems and networks, is a valuable asset to the Police Service. The ACPO/ACPOS Information Systems Community Security Policy (CSP) details the	Reduced	Low	Yes

		strategy for the security of information processes throughout the police community:- http://library.college.police.uk/docs/APPref/ACPO-ACPOS-2009-Information-Systems.pdf Her Majesty's Government (HMG) has published a Security Policy Framework which sets outs the expectations of how HMG organisations will apply protective security to ensure HMG can function effectively, efficiently and securely:- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf ACPO/ACPOS recognise that information, systems and networks, are valuable assets to the police community and that information, systems and networks must be safeguarded to ensure the service meets their statutory and regulatory responsibilities. The service meets these responsibilities by the implementation of the Community Security Policy (CSP):- http://www.acpo.police.uk/documents/information/2012/20120606-im-comm-security-policy.pdf The Security Policy Framework has a mandatory requirement that departments and agencies must have clear policies and processes for reporting, managing and resolving ICT security incidents. Based on this requirement and its adoption in the ACPO/ACPOS CSP, the service has developed a triage process to assess the incidents for reporting, establish on-going risk, and actions to prevent recurrence in order to provide an overall assessment of Information Assurance for the Police Service. As required in HMG InfoSec Standard No.2 - Risk Management and Accreditation of Information Systems, all Police Organisations must conduct a Risk Assessment and obtain the appropriate accreditation for their systems carrying Protectively Marked information. It is assumed that all systems connected to the CJX or GSI have the necessary accreditation in place.			
IOM users may have concerns	Failure to protect personal data can	Only individuals that should have a policing purpose are able	Reduced	Low	Yes

regarding the security of the data	result in non-compliance with GDPR, DPA and/or HRA (Right to respect for private/family life). Operational matters could be compromised as a result of ineffective security, leading to harm to individuals, organisation, investigation, bringing offenders to justice. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police. Loss of confidence by users of the systems.	to access the information. Sensitive operational information would not be shared on the partnership system. Where appropriate reference to an Athena record, custody record or CAD may be made to inform that further information exists The Information Management Business Area (IMBA) has a person of chief officer rank known as the Director of Information, who maintains a portfolio for data protection, freedom of information and records management. This role promotes compliance, consistency and a corporate approach across the police service. The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in their statutory responsibility to comply with the Data Protection Act, which can be found at: http://www.app.college.police.uk/app-content/information-management/data-protection/ Contained within the APP is guidance to forces on security issues: http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-seven-security-and-protective-measures Personnel Security Vetting is an important process for enhancing the integrity and security of the police community. The Association of Chief Police Officers (ACPO) and the Association of Chief Police Officers in Scotland (ACPOS) has published a National Vetting Policy for the Police Community to support that commitment:- http://www.acpo.police.uk/documents/workforce/2012/201205-wfdba-vetting-policy.pdf ACPO/ACPOS recognise that information, including the supporting processes, systems and networks, is a valuable asset to the Police Service. The ACPO/ACPOS Information Systems Community Security Policy (CSP) details the strategy for the security of information processes throughout			

		the police community:- http://library.college.police.uk/docs/APPref/ACPO-ACPOS-2009-Information-Systems.pdf Her Majesty's Government (HMG) has published a Security Policy Framework which sets outs the expectations of how HMG organisations will apply protective security to ensure HMG can function effectively, efficiently and securely:- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf ACPO/ACPOS recognise that information, systems and networks, are valuable assets to the police community and that information, systems and networks must be safeguarded to ensure the service meets their statutory and regulatory responsibilities. The service meets these responsibilities by the implementation of the Community Security Policy (CSP):- http://www.acpo.police.uk/documents/information/2012/201206-im-comm-security-policy.pdf The Security Policy Framework has a mandatory requirement that departments and agencies must have clear policies and processes for reporting, managing and resolving ICT security incidents. Based on this requirement and its adoption in the ACPO/ACPOS CSP, the service has developed a triage process to assess the incidents for reporting, establish on-going risk, and actions to prevent recurrence in order to provide an overall assessment of Information Assurance for the Police Service. As required in HMG InfoSec Standard No.2 - Risk Management and Accreditation of Information Systems, all Police Organisations must conduct a Risk Assessment and obtain the appropriate accreditation for their systems carrying Protectively Marked information. It is assumed that all systems connected to the CJX or GSI have the necessary accreditation in place.			
F. Review, Retention & Disposal					

Data subjects may have concerns regarding the length of time their personal data is being held and affecting their right to privacy.	Failure to protect personal data can result in non-compliance with GDPR DPA and/or HRA (Right to respect for private/family life). Operational matters could be compromised as a result of ineffective security, leading to harm to individuals, organisation, investigation, bringing offenders to justice. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	Information regarding the scheme is not held longer than is necessary for the purposes needed. The retention period is six years following scheme de-registration, which is in place due to civil litigation threshold. The Information Management Business Area (IMBA) has a person of chief officer rank known as the Director of Information, who maintains a portfolio for data protection, freedom of information and records management. This role promotes compliance, consistency and a corporate approach across the police service. The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in their statutory responsibility to comply with the Data Protection Act, found at: http://www.app.college.police.uk/app-content/information-management/data-protection/ Contained within the APP is guidance to forces on retention issues:- http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-5-retention The College of Policing has published the Information Management Authorised Professional Practice (APP) to assist forces with their data collection and recording responsibilities, which can be found at: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/ Readers are also asked to refer to Section G of this table – Subject Rights (explains the rights afforded to individuals by the Data Protection Act and the duties of organisations in this regard).	Reduced	Low	Yes
IOM users may have concerns that information is removed prematurely and	Failure to protect personal data can result in non-compliance with GDPR, DPA and/or	Information is retained for a policing purpose, if there is an operational requirement for the information it will not be removed prematurely. The original information i.e. Athena, PNC record will be retained in line with MoPI and National guidance and therefore will be available for DBS disclosures.	Reduced	Low	Yes

prejudicing operational policing matters and Disclosure and Barring decisions.	HRA (Right to respect for private/family life). Operational matters could be compromised as a result of premature weeding of information resulting in harm to individuals, organisation, investigations and bringing offenders to justice. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police. Loss of confidence by users of the systems.	The Information Management Business Area (IMBA) has a person of chief officer rank known as the Director of Information, who maintains a portfolio for data protection, freedom of information and records management. This role promotes compliance, consistency and a corporate approach across the police service. The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in their statutory responsibility to comply with the Data Protection Act, which can be found at: http://www.app.college.police.uk/app-content/information-management/data-protection/ Contained within the APP is guidance to forces on retention issues:- http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-5-retention The College of Policing has published the Information Management Authorised Professional Practice (APP) to assist forces with their data collection and recording responsibilities, which can be found at: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/			
Data subjects may have concerns regarding the reviewing of their personal data and whether the process is being undertaken appropriately.	Failure to protect review personal data can result in non-compliance with GDPR, DPA, HRA (Right to respect for private/family life) and the College of Policing APP Information Management.	The RRD schedule is available as part of the Information Charter on the Constabularies' websites. This will demonstrate retention periods and provide when reviews take place. Review of information in undertaken under the National Retention Assessment Criteria (NRAC). The Information Management Business Area (IMBA) has a person of chief officer rank known as the Director of Information, who maintains a portfolio for data protection,	Reduced	Low	Yes

	Operational matters could be compromised as a result of ineffective reviewing of information, resulting in harm to individuals, organisation, investigations and bringing offenders to justice. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	freedom of information and records management. This role promotes compliance, consistency and a corporate approach across the police service. The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in their statutory responsibility to comply with the Data Protection Act, which can be found at: http://www.app.college.police.uk/app-content/information-management/data-protection/ Contained within the APP is guidance to forces on retention issues:- http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-5-retention The College of Policing has published the Information Management Authorised Professional Practice (APP) to assist forces with their data collection and recording responsibilities, which can be found at: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/ Readers are also asked to refer to Section G of this table – Subject Rights (explains the rights afforded to individuals by the Data Protection Act and the duties of organisations in this regard).			
Data subjects may have concerns regarding the secure manner in which their personal data weeded.	Failure to protect review personal data can result in non-compliance with GDPR, DPA, HRA (Right to respect for private/family life) and the College of Policing APP Information Management. Operational matters could be compromised	The information currently held on ECINS should be weeded by the administrator of the system. The information is held electronically so should be disposed of securely. The Information Management Business Area (IMBA) has a person of chief officer rank known as the Director of Information, who maintains a portfolio for data protection, freedom of information and records management. This role promotes compliance, consistency and a corporate approach across the police service. The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in	Reduced	Low	Yes

	as a result of ineffective reviewing of information, resulting in harm to individuals, organisation, investigations and bringing offenders to justice. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	their statutory responsibility to comply with the Data Protection Act, which can be found at: http://www.app.college.police.uk/app-content/information-management/data-protection/ Contained within the APP is guidance to forces on retention issues:- http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-5-retention The College of Policing has published the Information Management Authorised Professional Practice (APP) to assist forces with their data collection and recording responsibilities, which can be found at: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/			
G. Subject Rights					
Data subjects may have concerns regarding the application of their statutory information rights under the DPA and FOIA.	Failure to respond to applications in a timely and comprehensive manner - can result in non-compliance with GDPR, DPA, HRA (Right to respect for private/family life) and the College of Policing APP Information Management. Operational matters could be compromised	All information held is searchable and retrievable to be able to fulfil individuals' rights under the DPA and FOIA. The Information Management Business Area (IMBA) has a person of chief officer rank known as the Director of Information, who maintains a portfolio for data protection, freedom of information and records management. This role promotes compliance, consistency and a corporate approach across the police service. The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in their statutory responsibility to comply with the Data Protection Act, which can be found at: http://www.app.college.police.uk/app-content/information-	Reduced	Low	Yes

	as a result of ineffective reviewing of information, resulting in harm to individuals, organisation, investigations and bringing offenders to justice. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	management/data-protection/ Contained within the APP is guidance to forces on data subject rights:- http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-six-rights-of-data-subjects The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in their statutory responsibility to comply with the Freedom of Information Act 2000 (FOIA), which can be found at: http://www.app.college.police.uk/app-content/information-management/freedom-of-information/			
IOM users may have concerns regarding the application of individual's applying their statutory rights under the GDPR and DPA – which may result in information being disclosed in advance of thorough assessment of impact on operational matters.	Operational matters could be compromised as a result of ineffective reviewing of information, resulting in harm to individuals, organisation, investigations and bringing offenders to justice. Associated reputational damage to forces including financial and legal risks. Loss of public	When requests are received by the Data Protection Team regarding an individual's right under the legislation, checks are always made with the officers involved to ensure that the disclosure of such information will not prejudice an investigation. The Information Management Business Area (IMBA) has a person of chief officer rank known as the Director of Information, who maintains a portfolio for data protection, freedom of information and records management. This role promotes compliance, consistency and a corporate approach across the police service. The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in their statutory responsibility to comply with the Data Protection Act, which can be found at: http://www.app.college.police.uk/app-content/information-	Reduced	Low	Yes

	confidence. Reluctance to provide information to the police. Loss of confidence by users of the systems.	management/data-protection/ Contained within the APP is guidance to forces on data subject rights:- http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-six-rights-of-data-subjects The College of Policing has published the Data Protection Authorised Professional Practice (APP) to assist forces in their statutory responsibility to comply with the Freedom of Information Act 2000 (FOIA), which can be found at: http://www.app.college.police.uk/app-content/information-management/freedom-of-information/			

10. Step 7 – Sign-Off and Record Outcomes

Item	Name / Date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead.
DPO advice provided:	Bethany Mortimer 20/11/2018	DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice: It is advised that the individuals that are part of the IOM Scheme are giving a Fair Processing Notice – this can be facilitated by the Information Charter on the Force external facing websites. It is also advised that a process for weeding of ECINS is achieved through the administrators of the system. This needs to be in place for when the retention periods are met and weeding is needed.		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	DPO	If your decision departs from individuals' views, you must explain your reasons.
Comments: The processing for this Scheme was already in place for the requirement to complete a DPIA. Consultation with internal stakeholders from Information Management was decided as appropriate. Guidance provided in relation to retention periods and information security.		

This DPIA will be kept under review by:	DPO and Insp Danny Kett	The DPO should also review ongoing compliance with DPIA.