Privacy Impact Assessment: Athena

Version: 1.0
Date: 29th May 2015
Author: Athena Information Management Group
Owner: Athena Business Design Authority

Document Control

Sign-Off Details	
Sign-Off Authorities	**Date**
Athena Business Design Authority	21 May 2015

Distribution List			
Name	**Role**	**Version**	**Date**
Hayley Youngs Kate Eade	Head of Information Management - Norfolk/Suffolk Constabularies Compliance Officer - Norfolk/Suffolk Constabularies	Draft 0.1	2 Dec 2014
Hayley Youngs Kate Eade	Head of Information Management - Norfolk/Suffolk Constabularies Compliance Officer - Norfolk/Suffolk Constabularies	Draft 0.2	18 Dec 2014
Hayley Youngs Andy Begent Kate Eade	Head of Information Management - Norfolk/Suffolk Constabularies Head of Information Management - Essex Police Compliance Officer - Norfolk/Suffolk Constabularies	Draft 0.3	30 Dec 2014
Hayley Youngs Andy Begent Kate Eade	Head of Information Management - Norfolk/Suffolk Constabularies Head of Information Management - Essex Police Compliance Officer - Norfolk/Suffolk Constabularies	Draft 0.4	6 Jan 2015
Hayley Youngs Kate Eade	Head of Information Management - Norfolk/Suffolk Constabularies Compliance Officer - Norfolk/Suffolk Constabularies	Draft 0.5	15 Jan 2015
Hayley Youngs Andy Begent Kate Eade	Head of Information Management - Norfolk/Suffolk Constabularies Head of Information Management - Essex Police Compliance Officer - Norfolk/Suffolk Constabularies	Draft 0.6	20 Jan 2015
Athena Information Management Group		Draft 0.7	4 Feb 2015
Athena Information Management Group		Draft 0.8	Feb 2015

Distribution List			
Name	**Role**	**Version**	**Date**
Athena Business Design Authority		0.9	May 2015
Athena Information Management Group and Athena Business Design Authority		1.0	29 May 2015

Version Control		
Version	**Date**	**Summary of Changes**
Draft 0.1	2 Dec 2014	New
Draft 0.2	18 Dec 2014	New
Draft 0.3	30 Dec 2014	Privacy Issues
Draft 0.4	6 Jan 2015	References to mitigation from Information Management Code of Connection
Draft 0.5	15 Jan 2015	Consistency of terminology, web links and completion of Step 2.
Draft 0.6	20 Jan 2015	Removal of non-relevant appendices & inclusion of additional text on Step 4-6
Draft 0.7	3 Feb 2015	Minor amendments of the Athena Information Management Group (AIMG)
Draft 0.8	4 Feb 2015	Minor amendments of the AIMG
Draft 0.9	5 May 2015	Inclusion of responses from the PIA consultation exercise for submission to the Athena Business Design Authority on 21 May 2015
1.0	29 May 2015	Finalised version reflecting decisions made by the Athena Business Design Authority on 21 May 2015

Contents

1. Executive Summary

1.1. Athena is a collaborative project across seven police forces, including Bedfordshire, Cambridgeshire, Essex, Hertfordshire, Kent, Norfolk and Suffolk constabularies to share a new IT system. The system will be referred to as Athena.

1.2. Athena will allow information to be managed effectively by enabling forces to share information across police boundaries in four key areas:

- Intelligence
- Investigation
- Managing offenders, and
- Preparing files for court.

1.3. It will align business processes for the use of Athena across all seven forces, which may drive further efficiencies and performance improvements. The wider implications for the Athena project are not confined to the initial seven forces. It is anticipated that the solution will have wider adoption across a number of UK police services and other law enforcement bodies as it develops.

1.4. This Privacy Impact Assessment (PIA) has been produced to help identify and assess data protection and privacy related issues concerning Athena.

1.5. Throughout the development of Athena an Information Management Group (AIMG) has advised the project on how information management issues including privacy might be addressed. A previous PIA was drafted earlier in the project and as a result, the AIMG produced an Information Management Code of Connection which documents many of the measures identified by the group and approved by the seven forces. The Information Management Code of Connection (IMCoCo) was formally approved and adopted by the Athena Business Design Authority (BDA)[1] on 22 November 2014 and a revised version issued on 16 April 2015.

1.6. This PIA is produced under the Information Commissioner's new template which was introduced sometime after the initial draft PIA was produced.

[1] Athena Business Design Authority (BDA) – Group that maintains tactical oversight of information management matters on behalf of members of Athena. Reports to the strategic Athena Information Management Board

2. Purpose of a PIA

2.1. The Privacy Impact Assessment (PIA) is a flexible process which assists organisation in identifying and minimising the privacy risks of new projects or policies. Conducting a PIA involves working with people within the organisation, with partner organisations and with the people affected to identify and reduce privacy risks. A PIA will help to ensure potential problems 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 Privacy Impact Assessment will aim to incorporate the following process:

- Identify the need for a PIA
- Describe the information flows;
- Identify the privacy and related risks;
- Identify and evaluate the privacy solutions;
- Sign-off and record the PIA outcomes
- Integrate the PIA outcomes into the project plan, and
- Consult with internal and external stakeholders as needed throughout the process.

2.3. The Conducting Privacy Impact Assessments - Code of Practice, launched by the Information Commissioner's Office (ICO) in February 2014 has been used to support this PIA.

3. Structure of this Document

This document explains:

- What Athena is, including its aims and benefits;
- How the steps from the Information Commissioners Conducting Privacy Impact Assessments Code of Practice have been addressed, including:

  Step 1 – Identify the Need for a Privacy Impact Assessment (PIA)

  Step 2 – The Information Flows and Consultation Requirements

  Step 3 – The Privacy and Related Risks

  Step 4 – The Privacy Solutions

  Step 5 – Sign Off of PIA Outcomes

  Step 6 – Integrate the PIA into the Project Plan

What is Athena?

3.1. Athena is a collaborative project involving seven police forces to share a new IT system. The system will contain the majority operational data owned by those forces and is known as Athena.

3.2. The project has been running for several years involving the seven forces and working alongside Northgate Information Solutions UK limited to develop the solution (Athena). Athena will continue to be developed with new functionality and changes to existing functions as operational needs arise, following go live in Essex (reference force) in 2015.

3.3. Northgate Information Solutions UK limited has been awarded the contract to centrally host Athena.

3.4. It is anticipated that wider adoption of Athena by police forces and law enforcement bodies may take place in the future.

3.5. **Athena Aims**:

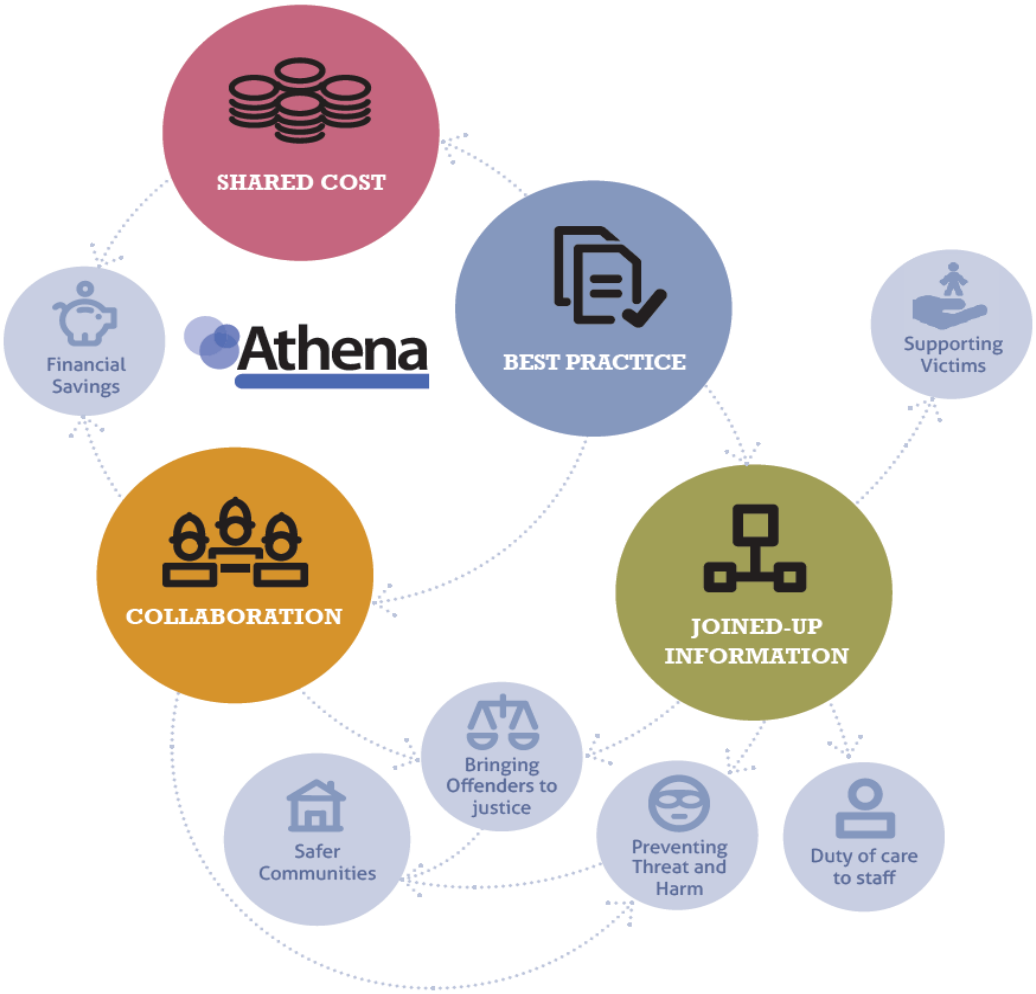
- To allow multiple forces to see across all information to create a safer environment for local communities.
- To help maintain investment in frontline policing by achieving savings through using one shared IT system.

3.6. **Athena Benefits:**

- Will enable each force to access more information about an individual thereby reducing the risk presented by cross border criminality and enable a fuller understanding of the risks presented by known criminals.
- Will help to reduce financial burden on forces at a time of austerity.
- Will enable consistent working practices to be adopted across multiple forces to provide a foundation for further collaboration between them.
- Will enable a more streamlined and effective approach to the manner in which information is recorded and managed in a shared system as identified by the Bichard Report[1] to help remove isolated 'silos' of information.

[1] http://dera.ioe.ac.uk/6394/1/report.pdf

- Will enable a more effective system with increased functionality to reduce re-keying, duplication and searching, thus enhancing time-saving opportunities, data quality and data management.



3.7. Athena will support local people by helping the police better protect the most vulnerable from harm, provide better support to witnesses through the justice process, and deliver faster justice for victims. Police Officers and staff alike will be better informed when talking to members of the public, building trust and confidence in local communities.

4. Step 1 - Identify the Need for a PIA

4.1. In accordance with the ICO Code of Practice an assessment was carried out to determine if a PIA was necessary using the following screening questions:-

- **Does the system involve multiple organisations whether they are government agencies or private sector organisations?**

  Yes. At present the intention is that Athena will only be used by forces that form part of the UK Police Service. However we do anticipate that Athena will be accessed beyond the police service by trusted partners that contribute to achieving the policing purpose e.g. as staff working on behalf of a police force in the context of custody doctors, Multi-agency Safeguarding Hubs, Victim Care. This is no different to current arrangements undertaken by forces.

- **Does the system involve new or significantly changed handling of personal data that is of particular concern to individuals?**

  No. The handling processes are consistent with existing practices albeit on a wider scale.

- **Does the project involve new or significantly changed handling of a considerable amount of personal data about individuals in the system?**

  Yes. Athena will change the way personal data is handled across the Athena forces. It will draw personal data about an individual from a wider range of sources, thus increasing the amount of personal data available about an individual.

- **Will the project involve the collection of new information about individuals?**

  No, the same information will be collected in accordance with UK Police Forces statutory and common law policing powers.

- **Will the project compel individuals to provide information about themselves?**

  Yes, however the information is no different to that which has always been provided to enable the police to exercise their lawful powers.

- **Will the information about individuals be disclosed to organisations or people who have not previously had routine access to information?**

  Yes. The system will enable wider access to information of the Athena forces. Previously access to another forces data tended to be on an ad hoc request basis, whereas Athena will enable improved availability to information to enhance policing. It is not thought Athena will increase the scope of the disclosure of information beyond the police than previous arrangements.

- **Does the system involve you using new technologies which might be perceived as being privacy intrusion?**

  No. Athena is a new cross-force, technical system for information collection, evaluation, dissemination and disposal. The opportunity for data mining is significant and users of the systems will have access to a broader demographic than previously available from a single force perspective.

  Whilst this represents a new collaborative way of working, it is not creating new or changing existing well established police business processes and activities. Athena will bring together existing information, which is currently held lawfully by a local force, into a single repository and will provide forces with a significantly improved understanding of the risks posed by individuals that operate across force boundaries.

  At present Athena will not use biometrics or facial recognition technologies.

- **Does the system involve new identifiers?**

  No. The system will reuse existing system identifiers from the various data feeds being provided by members of the Consortium. e.g. a Police National Computer (PNC) identification number will be reused to populate the designated field.

- **Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?**

  Yes. Athena system will link personal data on a wider scale across all forces. The data will be nominal centric enabling a wider collection of information to be known about a person.

  The system will change the way personal data is handled across Athena forces by linking personal data.

Athena forces will populate the system either from existing force information systems via a back record conversion process or with information as it becomes available.

The information entered by the force will then be cross-referenced, linked or merged with information already held within the system.

- **Does the system relate to data processing which is in any way exempt from legislative privacy protections?**

  No. All processing of personal data on the system will be covered by the Data Protection Act 1998 (DPA) and requires consideration of the Human Rights Act 1998 (HRA). The exemptions contained within the legislation will be applied where appropriate to do so, on a case-by-case basis.

- **Does the system involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?**

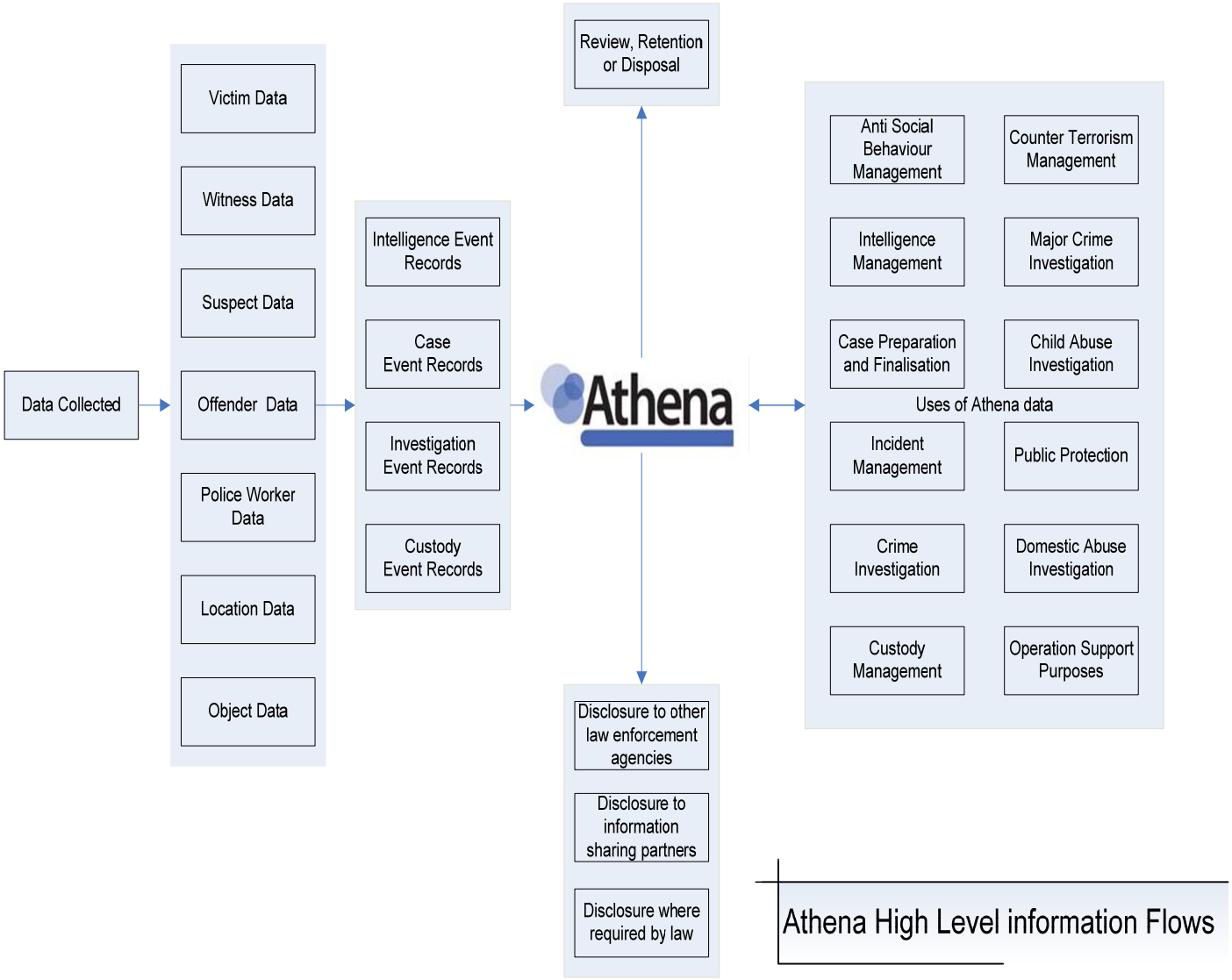
  No. General access to Athena will be restricted to forces who are members of the Athena Consortium and government partners who are subject to comparable privacy regulation. In addition, there will be access by the staff of other organisations that are contracted to work for Athena Consortium members. This access will be covered by the terms of data processing agreements/information sharing agreements and will be subject to the provisions of the Data Protection Act 1998.

4.2. In summary, there is nothing particularly new about the manner in which Athena requires police information to be used. The benefits of Athena will support forces to implement the recommendation following the Bichard Inquiry, which recognise intelligence gathering and improved information sharing across police force as a pre-requisite of modern effective policing. Also, there is a recognised public expectation that police forces will utilise police information to its full potential to improve public safety.

4.3. Arriving from the above screening questions, the advice of the ICO is that any questions resulting in a 'yes' answer would likely require a Privacy Impact Assessment to be carried out. As a result of Step 1 – it is recognised there is a requirement to further proceed with a PIA.

5. Step 2 - Information Flows

5.1 As part of the PIA process, organisations should describe how information is collected, stored, used, retained and deleted. The diagram below details the Athena high level information flows.



Athena High Level information Flows

5.2. How is information requested?

The power to request information comes in the main from the Police Acts and other pieces of legislation which enable police officers or police staff to carry out their duties, e.g. Police and Criminal Evidence Act 1984 (PACE), Criminal Procedures & Investigations Act 1996 (CPIA), etc. together with common law powers. The Police Act 1996, section 30(1) gives constables all the powers and privileges of a constable throughout England and Wales. Section 30(5) defines powers as powers under any enactment whenever passed or made. These powers

include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order. Under the Police Reform Act 2002, the chief officer can delegate certain powers to police staff. This ensures a consistent approach by the police forces in their legitimate data gathering objectives.

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/

5.3 How is information stored?

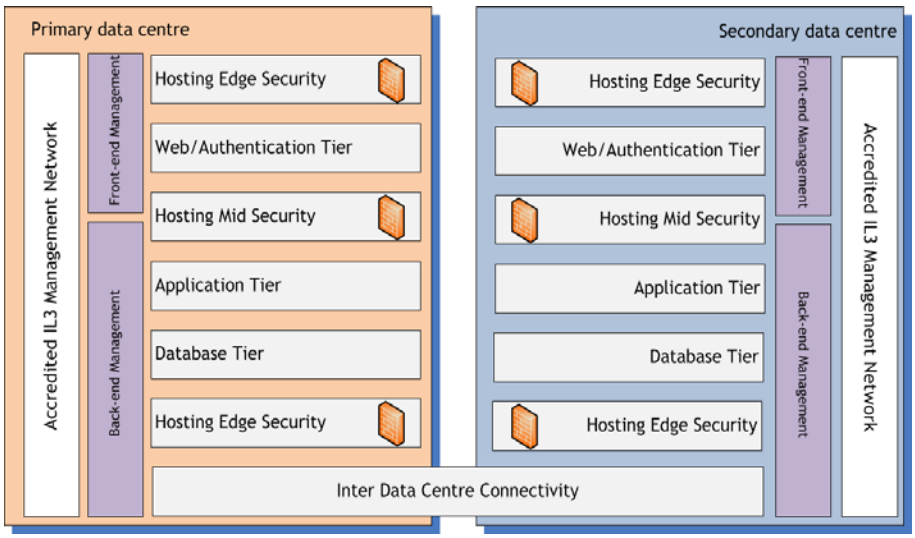
Athena is a service accessed over the internet via a secure private connection. In order to deliver the applications and associated services, the hosted infrastructure for Athena is based on a three tiered approach, to meet the requirements of IL3 protective marking:

- Web / Authentication tier
- Application tier
- Database tier

Each of these tiers is separated from external access by firewalls, and managed from the NPS IL3 secure management and backup networks.

A schematic overview of this approach is shown in the diagram below:

Athena Infrastructure Overview



The data is held in these two sites which are accredited to HMG government standards and approved as fit for purposes by the Home Office for use on their Private restricted network and will soon migrate over to the Public Services Network. The Athena project will deliver a standard Integrated Records Management System via a single hosted solution, allowing sharing of information across Police Forces, standardisation of business processes, improved operational performance and reduced costs. This will be implemented on a centrally hosted managed environment. Implementation and Management will be by Northgate IS.

5.4 How is information used?

Athena information will be used for policing purposes. The Code of Practice on the Management of Police Information [1] sets out at 2.2.2 that the police purposes are defined as; protecting life and property, preserving order, preventing the commission of offences, bringing offenders to justice and any duty or responsibility of the police arising from common or statute law.

5.5 How is information reviewed, retained and deleted?

Athena information will be reviewed in accordance with 4.5 – 4.6 of the Code of Practice on the Management of Police Information.

[1] http://library.college.police.uk/docs/homeoffice/codeofpracticefinal12073.pdf

6. Step 3 – Privacy and Related Risks

6.1. This chapter details the privacy issues, identified with Athena and how the risks will be managed.

6.2. Part of the process to identify the privacy issues were obtained following the compilation of a set of questions relating to compliance with the Data Protection Act.

Privacy Issue	Associated Risks	Mitigation
A. Obtaining		
Data subjects may feel their personal data is being obtained unfairly.	Non-compliance with the 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 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 1998, 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 obtaining by the police of personal data: http://www.app.college.police.uk/app-content/information-management/data-protection/#fair-processing-requirements-obtaining The IMCoCo – Chapter 7 – Appropriate Use of Athena Data sets out the justifications for how Athena data must be obtained, input, retained, disclosed or otherwise used. The IMCoCo- Chapter 12 – Fair Processing Notice/Information, encourages Athena Forces to publicly produce a Fair Processing notice. This is in keeping with the APP which requires forces to provide specific fair processing notices, when necessary: http://www.app.college.police.uk/app-content/information-management/data-protection/#police-use-of-fair-processing-notices

		Note: Under DPA Section 29(1), 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 power to request information comes in the main from the Police Act and other pieces of legislation which enable police officers or police staff to carry out their duties, e.g. Police and Criminal Evidence Act 1984 (PACE), Criminal Procedures Investigations Act 1996 (CPIA), etc. together with common law powers. The Police Act 1996, section 30(1) gives constables all the powers and privileges of a constable throughout England and Wales. Section 30(5) defines powers as powers under any enactment whenever passed or made. These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order. Under the Police Reform Act 2002, the chief officer can delegate certain powers to police staff. This ensures a consistent approach by the police forces in their legitimate data gathering objectives. 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 DPA and HRA. Associated reputational damage to forces including financial and legal risks. Loss of public confidence. Reluctance to provide information to the police.	Athena has been designed to capture relevant information with distinct inputting forms for business processes to permit a degree of granularity e.g. Custody would require the obtaining of medical details for the purpose of ensuring a safe detention, whereas the same information is unlikely to be obtained from a person reporting theft of property. 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 1998, 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 obtaining by the police of personal data: http://www.app.college.police.uk/app-content/information-management/data-protection/#fair-processing-requirements-obtaining The IMCoCo – Chapter 7 – Appropriate Use of Athena Data sets out the justifications for how Athena data must be obtained, input, retained, disclosed or otherwise used. The IMCoCo- Chapter 12 – Fair Processing Notice/Information, encourages Athena Forces to publicly produce a Fair Processing notice. This is in keeping with the APP which requires forces to provide specific fair processing notices, when necessary: http://www.app.college.police.uk/app-content/information-management/data-protection/#police-use-of-fair-processing-notices **Note**: Under DPA section 29(1), 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 power to request information comes in the main from the Police Act and other pieces of legislation which enable police officers or police staff to carry out their duties, e.g. Police and Criminal Evidence Act 1984 (PACE), Criminal Procedures Investigations Act 1996 (CPIA), etc. together with common law powers. The Police Act 1996, section 30(1) gives constables all the powers and privileges of a constable throughout England and Wales. Section 30(5) defines powers as powers under any enactment whenever passed or made. These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order. Under the Police Reform Act 2002, the chief officer can delegate certain powers to police staff. This ensures a consistent approach by the police forces in their legitimate data gathering objectives. 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 the Athena forces. Data subjects may feel the processing is a disproportionate intrusion of their privacy.	Non-compliance with the 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 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 1998, 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 The IMCoCo – Chapter 5.8 – Complaints and Disputes details how forces are obliged to consider any complaints or disputes raised by individuals over the processing (access, use, disclosure, retention, disposal etc.) of their personal data held on Athena. The IMCoCo – Chapter 6 – Data Processing sets out the conditions that forces must have in place with any person or organisation who is not employed by them who processes Athena data on their behalf. The IMCoCo – Chapter 7 – Appropriate Use of Athena Data sets out the justifications for how Athena data must be obtained, input, retained, disclosed or otherwise used. The IMCoCo – Chapter 8 – Misuse Management defines the way that misuse of Athena data is managed. The IMCoCo - Chapter 9 – Access Conditions sets out the conditions that forces and the AMO must comply with when determining whether access to Athena will be provided. The IMCoCo- Chapter 12 – Fair Processing Notice/Information, encourages Athena Forces to publicly produce a Fair Processing notice. This is in keeping with the APP which requires forces to provide specific fair processing notices, when necessary:

		http://www.app.college.police.uk/app-content/information-management/data-protection/#police-use-of-fair-processing-notices **Note**: Under DPA Section 29(1), 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. Within Athena the role profiles are developed and apportioned on a need to know (access to information basis). The IMCoCo – Chapter 18 – Audit & Compliance Activity sets out the various documents created to describe how Athena must be used by forces and the AMO. These included the Athena Standard Operating Procedures (which set out the business rules for the use of Athena) and the IMCoCo (which mandates how various information management-related matters involving Athena are managed). The IMCoCo – Chapter 19 – Transaction Validations sets out the activity that staff within the AMO and forces will undertake to validate a sample of overt transactions carried out by Athena Users on a regular and on-going basis. There will be a minimum level of transaction audit monitoring undertaken - Refer to 19.4.3 IMCoCo.
C. Disclosing		
Data subjects may have concerns regarding the disclosure of their personal data with the police service.	Non-compliance with the 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 suitability of Information Sharing Agreements is determined by Athena forces. Any initiatives involving external users of Athena will be determined by the Athena Management Organisation (AMO)[1]. 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/ The IMCoCo – Chapter 5.8 – Complaints and Disputes details how forces are obliged to consider any complaints or disputes raised by individuals over the processing (access, use, disclosure, retention, disposal etc.) of their personal data held on Athena. The IMCoCo – Chapter 5.10 – Civil Court Orders requiring disclosure of Athena Data details the process followed where forces receive a Court Order requiring the disclosure of Athena Data.

[1] Athena Management Organisation (AMO) – refer to 4.3.1 of the Athena Information Management Code of Connection

		The IMCoCo – Chapter 7 – Appropriate Use of Athena Data sets out the justifications for how Athena data must be obtained, input, retained, disclosed or otherwise used. The IMCoCo - Chapter 9 – Access Conditions sets out the conditions that forces and the AMO must comply with when determining whether access to Athena will be provided. The IMCoCo – Chapter 10 – User Understanding sets out the required information management related elements in any training/learning given to Users. The IMCoCo – Chapter 16 – Information Sharing sets out the principles underpinning the Athena approach to the sharing of data. The IMCoCo – Chapter 17.6 – Controls for External Users specifies a number of measures which apply to external users including the necessity to pass vetting to the Athena required standards before access to the system is authorised. The IMCoCo – Chapter 19 – Transaction Validations sets out the activity that staff within the AMO and forces will undertake to validate a sample of overt transactions carried out by Athena Users on a regular and on-going basis. There will be a minimum level of transaction audit monitoring undertaken - Refer to 19.4.3 IMCoCo.
Data subjects many have concerns regarding the disclosure of their personal data to partner agencies. E.g. Community Safety Partnerships	Non-compliance with the 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 suitability of Information Sharing Agreements is determined by Athena forces. Any initiatives involving external users of Athena will be determined by the Athena Management Organisation (AMO)[1]. 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/ The IMCoCo – Chapter 5.8 – Complaints and Disputes details how forces are obliged to consider any complaints or disputes raised by individuals over the processing (access, use, disclosure, retention, disposal etc.) of their personal data held on Athena. The IMCoCo – Chapter 7 – Appropriate Use of Athena Data sets out the justifications for how Athena data must be obtained, input, retained, disclosed or otherwise used.

[1] Athena Management Organisation (AMO) – refer to 4.3.1 of the Athena Information Management Code of Connection

		The IMCoCo - Chapter 9 – Access Conditions sets out the conditions that forces and the AMO must comply with when determining whether access to Athena will be provided. The IMCoCo – Chapter 10 – User Understanding sets out the required information management related elements in any training/learning given to Users. The IMCoCo – Chapter 16 – Information Sharing sets out the principles underpinning the Athena approach to the sharing of data. The IMCoCo – Chapter 17.6 – Controls for External Users specifies a number of measures which apply to external users including the necessity to pass vetting to the Athena required standards before access to the system is authorised. The IMCoCo – Chapter 19 – Transaction Validations sets out the activity that staff within the AMO and forces will undertake to validate a sample of overt transactions carried out by Athena Users on a regular and on-going basis. There will be a minimum level of transaction audit monitoring undertaken - Refer to 19.4.3 IMCoCo.
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 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 suitability of Information Sharing Agreements is determined by Athena forces. Any initiatives involving external users of Athena will be determined by the Athena Management Organisation (AMO)[1]. 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/ The IMCoCo – Chapter 5.8 – Complaints and Disputes details how forces are obliged to consider any complaints or disputes raised by individuals over the processing (access, use, disclosure, retention, disposal etc.) of their personal data held on Athena. The IMCoCo – Chapter 5.10 – Civil Court Orders requiring disclosure of Athena Data details the process followed where forces receive a Court Order requiring the disclosure of Athena Data. The IMCoCo – Chapter 7 – Appropriate Use of Athena Data sets out the justifications for how Athena data must be obtained, input, retained, disclosed or otherwise used. The IMCoCo - Chapter 9 – Access Conditions sets out the conditions that forces and the AMO must comply with when determining whether access to Athena will be provided.

[1] Athena Management Organisation (AMO) – refer to 4.3.1 of the Athena Information Management Code of Connection

		The IMCoCo – Chapter 10 – User Understanding sets out the required information management related elements in any training/learning given to Users. The IMCoCo – Chapter 16 – Information Sharing sets out the principles underpinning the Athena approach to the sharing of data. The IMCoCo – Chapter 17.6 – Controls for External Users specifies a number of measures which apply to external users including the necessity to pass vetting to the Athena required standards before access to the system is authorised. The IMCoCo – Chapter 19 – Transaction Validations sets out the activity that staff within the AMO and forces will undertake to validate a sample of overt transactions carried out by Athena Users on a regular and on-going basis. There will be a minimum level of transaction audit monitoring undertaken - Refer to 19.4.3 IMCoCo.
D. Data Quality		
Data subjects may have concerns regarding the accuracy, reliability, adequacy of their data	Non-compliance with the 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 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 1998, 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 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

		An Athena Data Quality Plan will be developed by the Athena Information Management Group[1] for forces to implement on at least an annual basis. The IMCoCo – Chapter 5.8 – Complaints and Disputes details how forces are obliged to consider any complaints or disputes raised by individuals over the data quality (accuracy, reliability, adequacy etc.) of their personal data held on Athena. The IMCoCo – Chapter 10 – User Understanding sets out the required information management related elements in any training/learning given to Users. The IMCoCo – Chapter 11 – Data Quality sets out how forces will ensure that data quality is achieved with any legacy data migrated into Athena and data input by users post go-live. The IMCoCo – Chapter 13 – Data Migration sets out the data migration principles to be adopted by forces to achieve consistency of approach. The IMCoCo - Chapter 14 – Matching and Merging of Records establishes the Match Rules developed by the AMO for the matching and automated merging of person records, object records and location records. The IMCoCo – Chapter 18 – Audit & Compliance Activity sets out the various documents created to describe how Athena must be used by forces and the AMO. These included the Athena Standard Operating Procedures (which set out the business rules for the use of Athena) and the IMCoCo (which mandates how various information management-related matters involving Athena are managed). The IMCoCo – Chapter 19 – Transaction Validations sets out the activity that staff within the AMO and forces will undertake to validate a sample of overt transactions carried out by Athena Users on a regular and on-going basis. There will be a minimum level of transaction audit monitoring undertaken - Refer to 19.4.3 IMCoCo. 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).
Athena users may have concerns regarding the accuracy, reliability, adequacy of their data	Non-compliance with the 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	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 1998, which can be found at:

[1] Athena Information Management Group (AIMG) – refer to 4.4.1 of the Athena Information Management Code of Connection

	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. Loss of confidence by users of the systems. Searching of the system will be more time consuming and further lead to correction reports.	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 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 An Athena Data Quality Plan will be developed by the Athena Information Management Group[1] for forces to implement on at least an annual basis. The IMCoCo – Chapter 10 – User Understanding sets out the required information management related elements in any training/learning given to Users. The IMCoCo – Chapter 11 – Data Quality sets out how forces will ensure that data quality is achieved with any legacy data migrated into Athena and data input by users post go-live. The IMCoCo – Chapter 13 – Data Migration sets out the data migration principles to be adopted by forces to achieve consistency of approach. The IMCoCo - Chapter 14 – Matching and Merging of Records establishes the Match Rules developed by the AMO for the matching and automated merging of person records, object records and location records. The IMCoCo – Chapter 18 – Audit & Compliance Activity sets out the various documents created to describe how Athena must be used by forces and the AMO. These included the Athena Standard Operating Procedures (which set out the business rules for the use of Athena) and the IMCoCo (which mandates how various information management-related matters involving Athena are managed). The IMCoCo – Chapter 19 – Transaction Validations sets out the activity that staff within the AMO and forces will undertake to validate a sample of overt transactions carried out by Athena Users on a regular and on-going basis. There will be a minimum level of transaction audit monitoring undertaken - Refer to 19.4.3 IMCoCo.

[1] Athena Information Management Group (AIMG) – refer to 4.4.1 of the Athena Information Management Code of Connection

		Through the AIMG any concerns regarding Data Quality are escalated to the Business Design Authority (BDA)[1] for further consideration.
E. Security		
Data subjects may have concerns regarding the security of their data	Failure to protect personal data can result in non-compliance with 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.	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 1998, 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 The IMCoCo – Chapter 6 – Data Processing sets out the conditions that forces must have in place with any person or organisation who is not employed by them who processes Athena data on their behalf. 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:-

[1] Athena Business Design Authority – refer to 4.2.1 of the Athena Information Management Code of Connection

		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. These Risk Management Accredited Documents Sets (RMADS) are protectively marked at RESTRICTED and are held centrally at the Home Office and the Athena Management Organisation located in Chelmsford.
Athena users may have concerns regarding the security of the data	Failure to protect personal data can result in non-compliance with 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.	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 1998, 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

	Loss of public confidence. Reluctance to provide information to the police. Loss of confidence by users of the systems.	The IMCoCo – Chapter 6 – Data Processing sets out the conditions that forces must have in place with any person or organisation who is not employed by them who processes Athena data on their behalf. 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. These Risk Management Accredited Documents Sets (RMADS) are protectively marked at RESTRICTED and are held centrally at the Home Office and the Athena Management Organisation located in Chelmsford.
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 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.	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 1998, 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/ The IMCoCo – Chapter 5.8 – Complaints and Disputes details how forces are obliged to consider any complaints or disputes raised by individuals over the processing (access, use, disclosure, retention, disposal etc.) of their personal data held on Athena. The IMCoCo – Chapter 15 – Retention and Disposal of Athena Data sets out how the retention/disposal of records from Athena will be managed in a manner compliant with the Data Protection Act 1998 and with regard to the College of Policing APP on Information Management (formerly Management of Police Information (MoPI) Guidance). 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 1998 and the duties of organisations in this regard).
Athena users may have concerns that information is removed prematurely and prejudicing operational policing matters and	Failure to protect personal data can result in non-compliance with DPA and/or HRA (Right to respect for private/family life).	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.

Disclosure and Barring decisions.	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 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 1998, 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/ The IMCoCo – Chapter 5.8.3 – Complaints and Disputes details how forces are obliged to consider any complaints or disputes raised by individuals over the processing (access, use, disclosure, retention, disposal etc.) of their personal data held on Athena. This section sets out the process agreed by forces when dealing with such cases. The IMCoCo – Chapter 7 – Appropriate Use of Athena Data sets out the justifications for how Athena data must be obtained, input, retained, disclosed or otherwise used. The IMCoCo – Chapter 15 – Retention and Disposal of Athena Data sets out how the retention/disposal of records from Athena will be managed in a manner compliant with the Data Protection Act 1998 and with regard to the College of Policing APP on Information Management (formerly Management of Police Information (MoPI) Guidance).
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 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,	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 1998, 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-

	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.	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/ The IMCoCo – Chapter 5.8 – Complaints and Disputes details how forces are obliged to consider any complaints or disputes raised by individuals over the processing (access, use, disclosure, retention, disposal etc.) of their personal data held on Athena. The IMCoCo – Chapter 15 – Retention and Disposal of Athena Data sets out how the retention/disposal of records from Athena will be managed in a manner compliant with the Data Protection Act 1998 and with regard to the College of Policing APP on Information Management (formerly Management of Police Information (MoPI) Guidance). The IMCoCo – Chapter 18 – Audit & Compliance Activity sets out the various documents created to describe how Athena must be used by forces and the AMO. These included the Athena Standard Operating Procedures (which set out the business rules for the use of Athena) and the IMCoCo (which mandates how various information management-related matters involving Athena are managed). The IMCoCo – Chapter 19 – Transaction Validations sets out the activity that staff within the AMO and forces will undertake to validate a sample of overt transactions carried out by Athena Users on a regular and on-going basis. There will be a minimum level of transaction audit monitoring undertaken - Refer to 19.4.3 IMCoCo. 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 1998 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 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	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 1998, 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

	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.	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/ The IMCoCo – Chapter 5.8 – Complaints and Disputes details how forces are obliged to consider any complaints or disputes raised by individuals over the processing (access, use, disclosure, retention, disposal etc.) of their personal data held on Athena. The IMCoCo – Chapter 15 – Retention and Disposal of Athena Data sets out how the retention/disposal of records from Athena will be managed in a manner compliant with the Data Protection Act 1998 and with regard to the College of Policing APP on Information Management (formerly Management of Police Information (MoPI) Guidance).
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 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.	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 1998, 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 data subject rights:- http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-six-rights-of-data-subjects The IMCoCo – Chapter 5.6 – Subject Access to Athena Data details how forces are legally obliged to respect and apply the right of subject access to Athena data. The IMCoCo – Chapter 5.7 – Data Subject Rights other than Subject Access details how forces are legally obliged upon request to apply any of the other rights available to individuals whose data is in Athena. The IMCoCo – Chapter 5.8 – Complaints and Disputes details how forces are obliged to consider any complaints or disputes raised by individuals over the

	Reluctance to provide information to the police.	processing (access, use, disclosure, retention, disposal etc.) of their personal data held on Athena. 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/ The IMCoCo – Chapter 5.9 – Freedom of Information Act Requests for Information concerning Athena sets out the process forces will follow when FOIA requests for information are received which encompass Athena or Athena data.
Athena users may have concerns regarding the application of individual's applying their statutory rights under the 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 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 1998, 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 data subject rights:- http://www.app.college.police.uk/app-content/information-management/data-protection/#principle-six-rights-of-data-subjects The IMCoCo – Chapter 5.6.5 – Subject Access to Athena Data details how forces are legally obliged to respect and apply the right of subject access to Athena data. This section sets out the process agreed by forces when dealing with such applications. The IMCoCo – Chapter 5.7.3 – Data Subject Rights other than Subject Access details how forces are legally obliged upon request to apply any of the other rights available to individuals whose data is in Athena. This section sets out the process agreed by forces when dealing with such applications. The IMCoCo – Chapter 5.8.3 – Complaints and Disputes details how forces are obliged to consider any complaints or disputes raised by individuals over the processing (access, use, disclosure, retention, disposal etc.) of their personal data held on Athena. This section sets out the process agreed by forces when dealing with such cases. The IMCoCo – Chapter 7 – Appropriate Use of Athena Data sets out the justifications for how Athena data must be obtained, input, retained, disclosed or

		otherwise used. 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/ The IMCoCo – Chapter 5.9 – Freedom of Information Act Requests for Information concerning Athena sets out the process forces will follow when FOIA requests for information are received which encompass Athena or Athena data.

7. Step 4 – The Privacy Solutions

7.1 The below organisations were invited to provide a formal response to the PIA consultation exercise:

- Suffolk – Independent Advisory Group
- Norfolk –Independent Advisory Group
- Cambs - Independent Advisory Group
- Herts - Independent Advisory Group
- Beds - Independent Advisory Group
- Essex - Independent Advisory Group
- Kent – Independent Advisory Group
- Information Commissioners Office
- Superintendents Association
- NACRO
- Unison
- Government Equalities Office
- Eastern region Police Federation
- Victim Support
- Youth Justice Board
- ACPO (Data Protection Officer)
- Her Majesty's Inspectorate of Constabularies (HMIC)Liberty

7.2 The below responses were received:

Information Commissioner's Office – 30/3/15

Thank you for providing a copy of the Athena Privacy Impact Assessment for consideration which, along with The Information Management Code of Connection (IMCoCo), identifies and assesses the data protection and privacy concerns attributed to the use of Athena. I have addressed the 4 questions below and provided a brief comment where applicable.

Does the PIA sufficiently address privacy concerns relating to the *collection* of personal data? Yes

From the PIA it appears that the information that is to be collected will remain the same, in accordance with UK Police Forces statutory and common law policing powers. The PIA makes good reference to the College of Policing's Data Protection Authorised Professional Practice (APP) which assists forces to comply with the Data Protection Act (DPA) 1998.

In keeping with the first principle, fair processing concerns attributed to data collection are addressed in the PIA by referencing (IMCoCo) Chapter 12 and APP guidance in relation to Police fair processing notices. Further the PIA makes reference to the collection of relevant and necessary information as stated in IMCoCo Chapter 7.

Does the PIA sufficiently address privacy concerns relating to the *use* of personal data? Yes

It appears that the handling processes within the Athena system will be consistent with existing practices, but on a wider scale. Within 'Step 1 – Identify the Need for a PIA', it states that Athena information will be used for policing purposes. Members should ensure that the processing of personal information is necessary and proportionate for the purpose or purposes of Athena. The PIA makes reference to (IMCoCo) Chapter 7, which outlines 'Appropriate Use of Athena Data', in order to minimise any risk of harm to data subjects, through the processing of personal data.

Does the PIA sufficiently address privacy concerns relating to the *disclosure* of personal data? Yes

The PIA references (IMCoCo) Chapter 16, which details Information Sharing Agreements between multiple members, previously established as separate 'silos'. In terms of external users of Athena, the PIA highlights the concern data subjects may have in relation to the disclosure of their personal data outside of the police service. In keeping with the seventh principle of the Data Protection Act (DPA) 1998, (IMCoCo) Chapter 16 explains the need for contracts and agreements for any data processors involved in the Athena system, to minimise any risk of harm to data subjects, in the event of disclosure to third parties.

Is there anything further that you wish to raise about the PIA?

Where the Athena IMCoCo/PIA makes reference to exemptions to the Data Protection Act (DPA) 1998, it may be useful to give an example. It is appreciated that the use of exemptions may be on a case by case basis.

Norfolk Constabulary – Independent Advisory Group (Chair) – 31/3/15

I am very pleased to attach my comments in response to your request. Thank you to you and your colleagues for providing this opportunity and please do let me know if you would like any further information or clarification.

Does the PIA sufficiently address privacy concerns relating to the collection of personal data? Yes.

From my reading of the various documents, the data collection procedures incorporate existing practice which already sufficiently addresses privacy concerns.

Does the PIA sufficiently address privacy concerns relating to the use of personal data? Yes.

From my reading of the various documents, the use of the data is based on existing practice which already sufficiently addresses concerns relating to the use of the data.

Does the PIA sufficiently address privacy concerns relating to the disclosure of personal data? Yes.

From my reading of the various documents, the disclosure of the data is based on existing practice which already sufficiently addresses concerns relating to the disclosure of personal data.

Is there anything further that you wish to raise about the PIA? Yes.

The ImCoCo sets out a range of audit and oversight procedures (Chapter 18 and Chapter 19.) There is no mention of any independent, external involvement. Under section 19.7. Oversight, would it be appropriate to state the potential to involve IAG, either with individual members being involved or in reporting to the IAG as a group, as part of the options under 19.7.3? This would serve to strengthen the Oversight process and strengthen transparency.

Kent Constabulary – Independent Advisory Group (Chair) – 30/3/15

Does the PIA sufficiently address privacy concerns relating to the collection of personal data? Yes

Does the PIA sufficiently address privacy concerns relating to the use of personal data? Yes

Does the PIA sufficiently address privacy concerns relating to the disclosure of personal data? Yes

Is there anything further that you wish to raise about the PIA? As long as the use of information and those who have access to it are bound by the constraints as laid out in the PIA I have no concerns.

Police Superintendents Association of England & Wales – 10/3/15

Thank you for the opportunity to comment on the Athena Privacy Impact Assessment, however we do not consider that we need to do so at this stage.

8. Step 5 – Sign-Off of PIA Outcomes

8.1 The first column of the table below sets out the suggested privacy solutions which were identified as a result of the consultation exercise set out in Chapter 7. These were discussed by the Athena Information Management Group which drafted recommendations for the Athena Business Design Authority (found in the middle column of the table) . Those recommendations were accepted by the Athena Business Design Authority on 21st May 2015 and as a consequence this finalised document was produced.

Suggested Privacy Solution	View and recommendation of the Athena Information Management Group	Decision of the Athena Business Design Authority
Where the Athena IMCoCo/PIA makes reference to exemptions to the Data Protection Act (DPA) 1998, it may be useful to give an example. It is appreciated that the use of exemptions may be on a case by case basis.	As the IMCoCo contains numerous links to the College of Policing Authorised Professional Practice on Data Protection which provides a number of exemptions the police can potentially rely upon, the Athena Information Management Group considered this was already covered.	The Business Design Authority accepted the view and recommendation of the Athena Information Management Group.
The IMCoCo sets out a range of audit and oversight procedures (Chapter 18 and Chapter 19.) There is no mention of any independent, external involvement. Under section 19.7. Oversight, would it be appropriate to state the potential to involve IAG, either with individual members being involved or in reporting to the IAG as a group, as part of the options under 19.7.3? This would	The Athena Information Management Group considered that as forces are already subject to external audit regimes including, Information Commissioner Voluntary audits, Her Majesty's Inspectorate of Constabularies (HMIC) and Independent external auditors, that this was already covered.	The Business Design Authority accepted the view and recommendation of the Athena Information Management Group.

serve to strengthen the Oversight process and strengthen transparency.		

9. Step 6 – Integrate the PIA into the Project

9.1 On 21st May 2015 the Athena Business Design Authority accepted the recommendations of the Athena Information Management Group, which meant that there was no requirement for further privacy measures at that time. The Athena Business Design Authority determined that this Privacy Impact Assessment should be reviewed once the seven founder forces had implemented Athena. That review will be initiated by the Athena Information Management Group.