PD 608	PRIVACY IMPACT ASSESSMENT (PIA)
Type of Document:	PROCEDURE
Version:	1.0
Registered Owner:	Chief Constable
Author:	Information Management Officer
Effective Date:	1st September 2012
Review Date:	1st January 2013
Replaces document (if applicable)	n/a
Linked Documents:	PS105 Information Management Policy

Functional owner

Signed: ..... **Date:** .....

Name: Simon Tovey – Head of Business and Finance

Post: .....

Authorised

Signed: ..... **Date:** .....

Name: DCC Paul Scarrott

Post: .....

Table of Contents

SECTION 1 VERSION CONTROL 2
SECTION 2 BACKGROUND 2
SECTION 3 AIMS / OBJECTIVES....3
SECTION 4 DETAILS....3
SECTION 5 LEGISLATIVE COMPLIANCE 5
APPENDICES....6
Appendix A - PRIVACY IMPACT ASSESSMENT (PIA) WORKFLOW 7
Appendix B - PIA Screening Process 8
Appendix C - PRIVACY IMPACT ASSESSMENT (PIA) 9
Appendix D - Preliminary Privacy Impact Assessment (PIA) Report 15

SECTION 1 VERSION CONTROL

Version No.	Date	Post Holder/Author	Post	Reason for Issue
1.0	8/8/2012	Glen Langford	Information Management Officer (IMO)	DRAFT
1.1	31/08/2012	Glen Langford	IMO	Emergency Issue

SECTION 2 BACKGROUND

2.1 The Origins/Background Information

A Privacy Impact Assessment (PIA) is a process, which will enable Nottinghamshire Police to identify and address the likely privacy impact of new policies, initiatives and projects. Whilst a PIA considers privacy issues on a wider scale than Data Protection compliance considerations, undertaking a PIA does not negate the need for Data Protection and Information Security compliance to be undertaken. Nor does a Data Protection or Information Security compliance check cover all PIA aspects.

The Information Commissioners Office (ICO) Handbook describes PIAs as “a means of addressing project risk as part of overall project management and that by performing a PIA early in a project, an organisation avoids problems being discovered at a later stage, when the costs of making significant changes will be much greater.”

PIAs should be carried out on proposed policies, initiatives and projects or when amendments are made to existing policies, initiatives and projects that involve the processing of any personal data.

2.2 Motivators/Driving Forces

Both the Data Protection Act, 1998 and the Information Assurance Maturity Model require Nottinghamshire Police to consider Privacy Impact Assessments as part of the initial phase of a new policy, project and / or initiative to ensure that privacy issues are considered. Privacy issues include the privacy of personal information (Data Protection Act, 1998); the privacy of the person (e.g. body searches, body scanning); the privacy of

personal behaviour (observations of what individuals do); and the privacy of personal communication.

SECTION 3 AIMS / OBJECTIVES

3.1 The Principles and Scope of the Procedure

The Procedure provides a process which will enable:
- The collection of sufficient information about a new process / initiative / IT system to allow a decision to be made as to whether a Privacy Impact Assessment (PIA) should be conducted.
- A decision about whether the PIA should be small scale or full scale.
- A PIA report to be drafted.
- Any privacy risks to be identified, documented and considered.

3.2 The aim of the procedure

The aim of the procedure is to provide Nottinghamshire Police with a PIA process to follow in respect of any new policy, project and / or initiative that is to be formally approved.

SECTION 4 DETAILS

4.1 General Principles of the Procedure

This procedure will assist staff to understand when a PIA is necessary and at what level, and should be considered at the starting stages when it can influence and identify risks.

The consultation phase is key, so focus should be on identifying the appropriate internal and external stakeholders and consulting effectively.

Do not conclude that there are no privacy risks with a policy, project or initiative. The report should show what risks were identified and how they will be mitigated. The Force should be arguing why an acceptable level of risk is justified, not just ignoring risks that are there.

4.2 Why undertake a PIA?

Undertaking a PIA will assist the Force by;
- Increasing public confidence in the way in which the Force collects and uses personal information.
- Allowing the Force to consider the legal basis for the new system, any obligation in relation to the collection of the personal data and any prohibitions on the use of the information.
- Preventing problems arising and hence avoiding subsequent expense and disruption.
- Assisting with risk management.
- Protecting the reputation of the Force.

4.3 Will all new policies / projects / initiatives require a full PIA?

No – an initial assessment of the privacy risk should be undertaken to determine what scale of PIA is necessary (See Appendix A).

Full scale PIA – an in-depth internal assessment of privacy risks and liabilities e.g. does a new IT system now require the use of personal data where previously it was purely statistical in nature.

Small scale PIA – a less formalised process e.g. replacement or enhancement for an existing personal data system or a proposal to collect personal data from a new source.

4.4 When should a PIA be undertaken?

If the Force is introducing a new policy / project or initiative or IT system or is making significant changes to a process / IT system, that has implications for the use of personal information, a PIA should be considered.

It could be undertaken at the same time as the assessment e.g. Equality Impact Assessment, or it could be considered separately. Initial data protection and information considerations are identified early in a project stage, the compliance checks are usually undertaken once the design has reached a detailed stage.

Initial PIA work should be undertaken prior to going to tender, i.e. at project initiation phase or its equivalent or the business case stage – certainly before decisions are made about the IT system / process or initiative. It may be appropriate to insert the initial PIA within a relevant contract.

To be effective, the PIA should be reviewed regularly at each new project phase and a review undertaken e.g. at a stage review (PRINCE methodology).

A PIA should not be undertaken retrospectively on an IT system or process already in place but can be introduced under any significant revisions. Appendix B provides a PIA screening process. Initial PIA reports should be revisited during various stages of the process.

4.5 Examples of new initiatives / IT Systems

These could be such as Home Office Data Hub (Staff data), Crime Mapping (Victim data), use of social networking sites, implementing a new or significantly changing an IT system or business process which will capture new categories / types of personal data.

4.6 What should a PIA document look like?

There is no set format and it is likely to depend on individual requirements. It is important to log issues raised and how they have been addressed, so the document should include the privacy risks and countermeasures (this supports legal compliance and will also be a reference document for any media statements required in the future). The final report should refer back to the initial PIA and reviews, provide an outline of the outstanding PIA

risks and refer to previous mitigated risks. The PIA is attached as Appendix C, together with a PIA report as Appendix D.

4.7 Who should conduct a PIA and who should be involved in the process?

The policy, project or initiative manager or similar should conduct the PIA.

4.8 Consultation

Who to consult is dependant on the type of information being collected and the reason for use. What is important is what can be gained by such consultation e.g. information, which will prevent problems arising at a later stage which could result in cost and disruption.

Must be consulted;
- Subject Matter experts e.g. Information Management.
- Information Security.
- Review, Retention and Disposal.
- IT Management (if relevant).

Should be consulted;
- Users.
- Federation / UNISON / Superintendent's Association.
- Owner of the system / process / initiative (and any owners of systems it may impact on).
- Partner Agencies.
- Public (dependant on type).
- Regulatory Authorities e.g. Information Commissioners Office.

4.9 Responsibilities

The Senior Information Risk Owner (SIRO) should ensure that a PIA is completed at the appropriate stages of a project as it informs on risk assessments and risk management and then the SIRO should accept / reject any risk from the PIA document.

The policy, project or initiative owner should identify the individual who will conduct the PIA and ensure sufficient resources are provided to the PIA process. They should also complete the PIA tasks at appropriate times and be responsible for the Risk Register, which should include the PIA risks.

The PIA responsible person should complete the PIA and draft the PIA report.

SECTION 5 LEGISLATIVE COMPLIANCE

This document has been drafted to comply with the general and specific duties in the Equality Act 2010; Data Protection Act; Freedom of Information Act; European Convention of Human Rights; Employment Act 2002; Employment Relations Act 1999, and other legislation relevant to policing.

APPENDICES

Appendix A – PIA Workflow
Appendix B – PIA Screening Process
Appendix C – PIA
Appendix D – PIA Report

APPENDIX A - PRIVACY IMPACT ASSESSMENT (PIA) WORKFLOW

Prepare an initial assessment of the project / initiative that includes a project outline, stakeholder analysis and environmental scan.

↓

Discuss with IM and IS who will advise if more information is required.

↓

Initial screening with IM and IS informed by discussions.

↓

Carry out the PIA screening process (Appendix B and Flowchart) in consultation with IM and IS informed by discussions, to identify whether full or small scale PIA required and whether legislative compliance checks should be integrated into the overall project schedule. It would be appropriate to highlight any potential legislative compliance issues that may be apparent, at this early stage, although the full legislative compliance checks are normally carried out at a later stage of the project after the system design, business processes and rules have been specified sufficiently so that they can be assessed for compliance with the law.

↓

Preliminary PIA report (Appendix C)
(to all formal decisions regarding small scale or full scale PIA).

↓

Complete Small Scale / Full Scale PIA to include drafting report.

↓

Regular review of PIA plus data protection & information security requirements.

↓

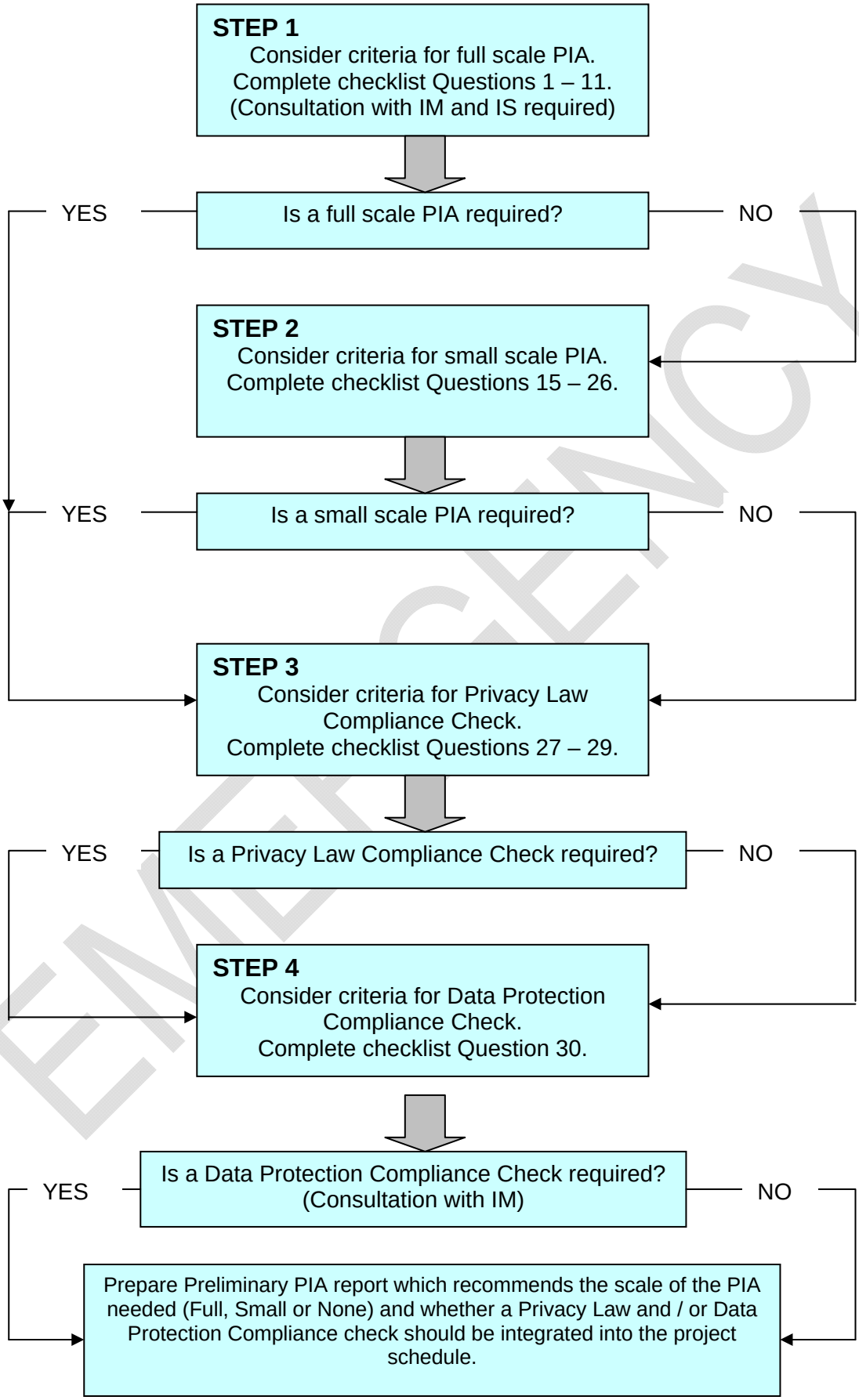
Consideration of risks from the PIA / DP and information security reviews to be included with Force Risk Register.

↓

PIA document plus risks presented to the SIRO (Information Assurance Board)

Abbreviations; IM – Information Management
IS – Information Security
PIA – Privacy Impact Assessment
DP – Data Protection
SIRO – Senior Information Risk Owner (Deputy Chief Constable)

APPENDIX B - PIA SCREENING PROCESS



APPENDIX C - PRIVACY IMPACT ASSESSMENT (PIA)

The answers to these questions will determine the scale of the PIA needed (Full, Small or None), and whether a Privacy Law and / or Data Protection Act compliance check is also required.

Policy / Project / Initiative -			
STEP 1 – CRITERIA FOR FULL SCALE PIA		**Yes**	**No**
	Technology		
1	**Does the work area apply new or additional information technologies that have substantial potential for privacy intrusion?** *Examples include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic.*	☐	☐
IDENTITY			
2	**Does the work area involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?** *Examples of relevant features include a digital signature initiative, a multi-purpose identifier, interviews and the presentation of identity documents as part of a registration scheme, and an intrusive identifier such as biometrics. All schemes of this nature have considerable potential for privacy impact and give rise to substantial public concern and hence risk.*	☐	☐
3	**Might the work area have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?** *Many police functions cannot be effectively performed without access to the client's identity. On the other hand, many others do not require identity. An important aspect of privacy protection is sustaining the right to interact with organisations without declaring one's identity.*	☐	☐
MULTIPLE ORGANISATIONS			
4	**Does the work area involve multiple organisations, whether they are government agencies (e.g. 'joined-up government' initiatives) or private sector organisations (e.g. ad outsourced service providers or as 'business partners')?** *Schemes of this nature often involve the breakdown of personal data silos and identity silos, and may raise questions about how to comply with data protection legislation. This breakdown may be desirable for fraud detection and prevention, and in some cases for business process efficiency. However, data silos and identity silos are of long standing, and have in many cases provided effective privacy protection. Particular care is therefore needed in relation to preparation of a business case that justifies the privacy invasions of projects involving multiple organisations. Compensatory protection measures should be considered.*	☐	☐
DATA			
5	**Does the work area involve new or significantly changed handling of personal data that is of particular concern to individuals?** The Data Protection Act (schedule 2) identifies a number of categories of 'sensitive personal data' that requires special care. These include racial and ethnic origin, political opinions, religious beliefs, trade union memberships, health conditions, sexual life, offences and court proceedings. *There are other categories of personal data that may not give rise to concerns, including financial data, particular data about vulnerable individuals, and data, which enable identity theft.* *Further important examples apply in particular circumstances. The addresses and phone numbers of a small proportion of the population need to be suppressed, at least at particular times in their lives, because such 'persons at risk' may suffer physical harm if they are found.*	☐	☐

6	**Does the work area involve new or significantly change handling of a considerable amount of personal data about each individual in the database?** *Examples include intensive data processing such as Staff HR, Crime data, and Intelligence data.*	☐	☐
7	**Does the work area involve new or significantly changed handling of personal data about a large number of individuals?** *Any data processing of this nature is attractive to organisations and individuals seeking to locate people, or to build or enhance profiles of them.*	☐	☐
8	**Does the work area involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?** *This is an especially important factor. Issues arise in relation to data quality, the diverse meanings of superficially similar data-items, and the retention of data beyond the very short term.*	☐	☐
EXEMPTIONS AND EXCEPTIONS			
9	**Does the work area relate to data processing, which is in any way exempt from legislative privacy protections?** *Examples include law enforcement and national security information systems and also other schemes where some or all of the privacy protections may be negated by legislative exemptions or exceptions.*	☐	☐
10	**Does the work area's justification include significant contributions to public security measures?** *Measures to address concerns about critical infrastructure and the physical safety of the population usually have a substantial impact on privacy. Yet there have been tendencies in recent years not to give privacy its due weight. This has resulted in tensions with privacy interests, and creates the risk of public opposition and non-adoption of the programme or scheme.*	☐	☐
11	**Does the work area involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?** *Disclosure may arise through various mechanisms such as information sharing with other agencies or outsourcing of aspects of the data-handling to sub-contractors.* *Third parties may not be subject to comparable privacy regulation because they are not subject to the provisions of the Data Protection Act or other statutory provisions, such as where they are in foreign jurisdiction. Concern may also arise in the case of organisations within the UK, which are subsidiaries of organisations headquartered outside the UK.*	☐	☐

The answers to questions 1 – 11 need to be considered as a whole to determine whether a full-scale PIA is warranted, and if so, whether the scope of the PIA should be wide-ranging or focused on a particular aspect of the project.

	Yes	No
Has IM and IS been consulted on this assessment?	☐	☐
FULL-SCALE PIA REQUIRED? **Please provide your reasoning –**	☐	☐

If a full-scale PIA is not required, proceed to <u>Step 2 – Criteria for Small Scale PIA</u>

<u>If a full-scale PIA is required, what should be its scope?</u>

<<NOT PROTECTIVELY MARKED>>

Proceed to <u>Step 3 – Criteria for Privacy Law Compliance Check</u>

Policy / Project / Initiative			
STEP 2 – CRITERIA FOR SMALL SCALE PIA		**Yes**	**No**
	Technology		
12	**Does the work area involve new or inherently privacy-invasive technologies?** *Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic.* *Technologies that are inherently intrusive, and technologies that are new and sound threatening, excite considerable public concern, and hence represent project risk.* *In order to answer this question, considerations include:* • *Whether all of the information technologies that are to be applied in the work area are already well-understood by the public:* • *Whether their privacy impacts are all well-understood by the Force, and by the public:* • *Whether there are established measures that avoid negative privacy impacts, or at least reduce them to the satisfaction of those whose privacy is affected:* • *And whether all of those measures are being applied in the design of the work area.*	☐	☐
JUSTIFICATION			
13	**Is the justification for the new data-handling unclear or UNPUBLISHED?** *Individuals are generally much more accepting of measures, even measures that are somewhat privacy-intrusive, if they can see that the loss of privacy is balanced by some other benefits to themselves or society as a whole. On the other hand, vague assertions that the measures are needed 'for security reasons', or 'to prevent fraud', are much less likely to calm public disquiet.*	☐	☐
IDENTITY			
14	**Does the work area involve an additional use of an existing identifier?**	☐	☐
15	**Does the work area involve use of a new identifier for multiple purposes?**	☐	☐
16	**Does the work area involve new or substantially changed identity authentication requirements that may be intrusive or onerous?** *The public understands that an identifier enables an organisation to collate data about an individual, and that identifiers that are used for multiple purposes enable data consolidation. They are also aware of the increasingly onerous registration processes and document production requirements imposed by organisations in recent years. From the perspective of the work area owner, these are warning signs of potential privacy risks.*	☐	☐
DATA			
17	**Will the work area result in the handling of a significant amount of new data about each person, or significant change in existing data-holdings?**	☐	☐
18	**Will the work area result in the handling of new data about a significant number of people, or a significant change in the population coverage?**	☐	☐
19	**Does the WORK AREA involve new linkage of personal data with data in other collections, or significant change in data linkages?**	☐	☐

	The degree of concern about a work area is higher where data is transferred out of its original context. The term 'linkage' encompasses many kinds of activities, such as the transfer of data, the consolidation of data-holdings, the storage of identifiers used in other systems in order to facilitate the future searches of the current content of records, the act of fetching data from another location (e.g. to support so-called 'front-end verification'), and the matching of personal data from multiple sources.		
DATA HANDLING			
20	**Does the work area involve new or changed data collection policies or practices that may be unclear or intrusive?**	☐	☐
21	**Does the work area involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory?**	☐	☐
22	**Does the work area involve new or changed data security arrangements that may be unclear or unsatisfactory?**	☐	☐
23	**Does the work area involve new or changed data access or disclosure arrangements that may be unclear or permissive?**	☐	☐
24	**Does the work area involve new or changed data retention arrangements that may be unclear or extensive?**	☐	☐
25	**Does the work area involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?**	☐	☐
EXEMPTIONS			
26	**Will the work area give rise to new or changed data handling that is in any way exempt from legislative privacy protection?**	☐	☐

Where the answers to questions 12 – 26 ore "Yes", consideration should be given to the extent of the privacy impact and the resulting project risk. The greater the significance, the more likely that a small-scale PIA is warranted.

If only one or two aspects give rise to privacy concerns, a small-scale PIA may still be justified. In these circumstances the PIA process should be designed to focus on the areas of concern. If on the other hand, multiple questions are answered "Yes", a more comprehensive assessment is appropriate.

	Yes	No
SMALL -SCALE PIA REQUIRED?	☐	☐

If a small-scale PIA is not required proceed to <u>Step 3 – Criteria for Privacy Law Compliance Check.</u>

<u>If a small-scale PIA is required, what should be its scope?</u>

Proceed to <u>Step 3 – Criteria for Privacy Law Compliance Check</u>

The answers to these questions will determine whether a privacy law compliance check will be required.

Policy / Project / Initiative			
STEP 3 – CRITERIA FOR PRIVACY LAW COMPLIANCE CHECK		**Yes**	**No**
27	**Does the work area involve any activities (including any data handling), that are subject to privacy or related provisions of any statute or other forms of regulation other than the Data Protection Act?** *In particular, the following laws and other forms of regulation should be considered, but the list may not be exhaustive:* • *The Human Rights Act, in particular Schedule 1, Article 8 (right to respect for private and family life) and Article 14 (prohibition of discrimination).* • *The Regulation of Investigatory Powers Act 2000 (RIPA) and Lawful Business Practice Regulations 2000.* • *The Privacy and Electronic Communications Regulations 2003 (PECR).* • *The Data Retention (EC Directive) Regulations 2007.* • *In the case of government agencies, the statutes under which the agency or programme operates.* • *Statues that impose regulatory conditions on the manner in which the organisation operates.* • *Sectoral legislation, e.g. Financial Services and Markets Act 2000.* • *Statutory codes, e.g. the Information Commissioner's CCTV code of practice.* *Where work areas are cross-jurisdictional the law of more than one country may be involved and other legal provisions may also need to be considered.*	☐	☐
28	**Does the work area involve any activities (including data handling) that are subject to common law constraints relevant to privacy?** *In particular, the following should be considered:* • *Confidential data relating to a person, as that term would be understood under the common law of confidence.* • *The tort of privacy as it develops through case law.*	☐	☐
29	**Does the work area involve any activities (including data handling) that are subject to less formal good practice requirements relevant to privacy?** *In particular, the following should be considered:* • *Industry standards, e.g. the BS ISO / IEC 17799:2005 Information Security Standard.*	☐	☐

If any of the questions 27 – 29 are answered "Yes", then a privacy law compliance check should be integrated into the project schedule.

Proceed to <u>Step 4 – Criteria for Data Protection Compliance Check</u>

The answers to these questions will determine whether a Data Protection compliance check will be required.

Policy / Project / Initiative			
STEP 4 – CRITERIA FOR DATA PROTECTION COMPLIANCE CHECK		**Yes**	**No**
30	**Does the work area involve the handling of any data that is <u>personal data</u>, as that term is used in the <u>Data Protection Act</u>?** *'Personal data' means data which relates to a living individual who can be identified:* *(a) from those data, or* *(b) from those data and other information which is in the possession of, or is likely to come into the possession of the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (Data Protection Act, s.1).* *Before proceeding to Data Protection Compliance checking, it is advisable to return to the screening process and review the outcomes of the four steps.* *Note that, where a PIA is needed, it should be commenced at an early stage of the overall work area, whereas compliance checking activities are usually conducted only once a fairly mature stage of business process design has been reached but not too late that it would significantly affect the project.*	☐	☐

If question 30 is answered "Yes", then a Data Protection Compliance Check should be integrated into the work area schedule.
Data Protection Compliance should be carried out in consultation with the Information Management Department.

Note that compliance checking activities are usually conducted reasonably late in the overall work area schedule, once detailed information about business processes and business rules are available.

PIA Screening Process completed by;

Name……

Signature……..

Date……

Reviewed by;

Name…….. **Name……**

Signature…….. **Signature……**

Date…… **Date……..**

APPENDIX D - PRELIMINARY PRIVACY IMPACT ASSESSMENT (PIA) REPORT

Purpose

The purpose of the report is to document the conduct of, and recommendations arising from the preliminary PIA process. The report is for the consideration of the Senior Information Risk Officer and should identify:

- Potential privacy and Data Protection risks related to the proposed work area.
- The scale of PIA required, (Full, Small or None).
- The scope of the PIA if one is required.
- Whether a privacy law compliance check should be integrated into the work area schedule.
- Whether a Data Protection compliance check should be integrated into the project schedule.

Format

The format of the report should be in accordance with local requirements. Where privacy and data protection risks have been identified, it is recommended that these are recorded in a format suitable for incorporation into the work area's Risk Register and / or Force Risk Register as appropriate.

Protective Marking – would suggest that this is marked as RESTRICTED when complete – however, that is for the originator to decide.

Structure and Content

The following elements are recommended and the level of detail should be adapted to suit the scope and complexity of the work area, and the level of risk identified.

Executive Summary:	An overview of the preliminary PIA process, including work area outline, stakeholder analysis, environmental scan, PIA screening results; and a summary of the main findings and recommendations.
Introduction:	The purpose of the preliminary PIA, the system / process to which it refers and any relationships with other internal / external systems / processes.
Work Area Background:	Work area description, purpose, scope, links to other work areas, stakeholders, type(s) of information to be processed, the reasons for processing and related privacy aspects.
Legislative & Policy authorities:	Record all known legislative and Police policies that are relevant to the work area.
Description of personal information:	What specific information is to be processed and how will it flow internally and externally. How will it be collected, used, stored, transferred and disclosed. What are the arrangements regarding subject access and data quality. Data elements and data flows should be described and / or mapped in relation to the identified stakeholders.
Potential privacy risks:	Privacy risks that have been identified and how these will affect stakeholders and the aims of the work area. The relevant seriousness of these risks and steps that might be taken to remove, mitigate or manage those risks.
Potential Data Protection risks:	Data Protection risks that have been identified and how these will affect stakeholders and the aims of the work area. The relevant seriousness of these risks and steps that might be taken to remove, mitigate or manage those risks.

Security Requirements:	Measures to protect personal information from loss and unauthorised access, use, modification or disclosure. Measures to protect personal information, which is transferred to other locations, and / or will be handled by external agencies. Review retention and disposal arrangements. Breach management policy.
Environmental:	Detail any consideration of prior PIAs within the organisation or in other organisations, consultations with other professional bodies, privacy regulators etc.
Recommendations:	These will be derived from the PIA screening process and should address whether a PIA is required, and if so what scale (Full or Small) and scope is appropriate. The recommendations should also address whether a privacy law compliance check and / or Data Protection Act compliance check should be integrated into the work area schedule. If a PIA is to be conducted the recommendations should include an indication of future activities, timescales and resource requirements for conducting the PIA. Where a PIA is needed it should be commenced at an early stage of the overall work area, whereas compliance checking activities are usually conducted at a much later stage, once detailed information about the business process design and business rules are available.