Information Security Document

Privacy Impact Assessment Procedures

Version 5.0

Version History			
Version	**Date**	**Detail**	**Author**
1.0	15/06/2017	First Draft for consideration by working group	Simon Hobbs
1.1	29/06/2017	Revised version for consideration by working group	Simon Hobbs
1.2	30/06/2017	Post working group version	Simon Hobbs
1.3	11/07/2017	Post IGG version	Simon Hobbs
1.4	26/11/2017	Post workshops and ICO Audit consultation version	Simon Hobbs
2.0	08/01/2018	Approved by Information Governance Group.	Simon Hobbs
3.0	07/02/2018	EDRM links added and Compliance Risk column deleted.	Simon Hobbs
4.0	25/03/2018	Amended to take account of GDPR requirements (ICO GDPR DPIA Guidance Consultation version 22nd March 2018) as well as further feedback from workshops	Simon Hobbs
5.0	14/05/2018	Minor amendments following workshops and GDPR changes.	Simon Hobbs

This document has been prepared using the following ISO27001:2013 standard controls as reference:	
ISO Control	**Description**
A.18.1.1	Identification of applicable legislation and contractual requirements
A.18.1.3	Protection of records
A.18.1.4	Privacy and Protection of personally identifiable information

CONTENTS

Contents	Page
Introduction	4
What is a Privacy Impact Assessment (PIA)?	4
When will a PIA be appropriate?	4-5
What is meant by Privacy?	5
Informational Privacy Risk	5-6
The Benefits of a PIA	6
Projects which might require a PIA	7
PIA Procedure	7
Monitoring	7

1. Introduction

A privacy impact assessment (PIA), also known as a data protection impact assessment (DPIA) is a tool which can help the Council identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

An effective PIA will allow the Council to identify and fix problems at an early project stage, reducing the associated costs and damage to reputation which might otherwise occur. From May 2018 a PIA will be mandatory in certain circumstances

This policy explains the principles which form the basis for a PIA.

The main body of the policy sets out the basic steps which the Council should carry out during the assessment process. A flowchart summarising the process is at Appendix 1.

Templates are available at Appendix 2. Annexes A, B and C EDRM Privacy Impact Assessments. In addition a Guidance Document has been created and is available at Privacy Impact Assessment Guidance. In the event of any doubt as to the implications of a project for the Council's compliance with data protection principles, then advice should be sought from Legal Services in the normal way.

Advice may also be sought from the Council's Data Protection Officer.

2. What is a Privacy Impact Assessment?

A PIA is a process which helps an organisation to identify and reduce the privacy risks of any project.

The PIA process is not new to the Council. Privacy implications are already considered as part of the project planning process. However, the aim of this procedure is to ensure that this is done on a systematic and consistent basis. The Council commenced formal PIAs in July 2017 and they are now embedded into procurement processes.

To be effective a PIA should be used throughout the development and implementation of a project, using existing project management processes.

A PIA will enable the Council to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

3. When will a PIA be appropriate?

PIAs will be applied to new projects and data sharing arrangements, because this allows greater scope for influencing how the project will be implemented.

A PIA can also be useful when planning changes to an existing system.

A PIA can also be used to review an existing system, but the organisation needs to ensure that there is a realistic opportunity for the process to implement necessary changes to the system. However, the Council does not propose to review existing systems, except as may be required under GDPR. Under GDPR there will be a requirement to carry out a PIA where there is a high risk to individuals. This is reflected in the screening questions at Appendix 2. Since however it is good practice do a PIA for major new projects the Council's policy as set out in this procedure is likely to exceed the strict legal requirements.

The main purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met.

Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice.

This analysis can be tested by consulting with people who will be working on, or affected by, the project including the project team itself. Exceptionally where for example the privacy risks are considered to be high consultation with the wider public may be appropriate. In the case of new data sharing agreements consultation with the partners involved would be good practice.

Conducting a PIA does not have to be complex or time consuming but there must be a level of rigour in proportion to the privacy risks arising.

A PIA should be completed before a project is undertaken. Please refer to the flowchart at Appendix 1.

4. What is meant by Privacy?

Privacy, in its broadest sense, is about the right of an individual to be left alone.

It can take two main forms, and these can be subject to different types of intrusion:

- Physical privacy - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, body searches or other interference, acts of surveillance and the taking of biometric information.
- Informational privacy – the ability of a person to control, edit, manage and delete information about them and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and

extends to monitoring the records of senders and recipients as well as the content of messages
.

5. Informational Privacy

This policy is concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information.

Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to someone where the person who it is about does not want them to have it;
- used in ways that are unacceptable to or unexpected by the person it is about; or
- not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information.

Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised. There is also harm which goes beyond the immediate impact on individuals. The harm arising from use of personal information may be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. It might for example contribute to a loss of personal autonomy or dignity or exacerbate fears of excessive surveillance.

The outcome of a PIA should be a minimisation of privacy risk.

6. The legal duty to carry out a PIA and the benefits of a PIA

The Information Commissioner (ICO) promotes PIAs as a tool which will help organisations to comply with their DPA obligations, as well as bringing further benefits.

Conducting a PIA is a legal requirement of the GDPR in certain limited circumstances where there is a high risk to privacy, but carrying out an effective PIA should also benefit the people affected by a project and also the organisation carrying out the project. Additionally it is a requirement of the Information Governance Toolkit Assessment to show that PIAs are undertaken.

A PIA will be legally required where the Council plans to;

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Process special category data or criminal offence data on a large scale.
- Systematically monitor a publicly accessible place on a large scale.
- Use new technologies.
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- Carry out profiling on a large scale.
- Process biometric or genetic data.
- Combine, compare or match data from multiple sources.
- Process personal data without providing a privacy notice directly to the individual.
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- Process personal data which could result in a risk of physical harm in the event of a security breach

Conducting and publicising a PIA will help the Council to build trust with the people using their services.

There can be financial benefits to conducting a PIA. Identifying a problem early will generally require a simpler and less costly solution. A PIA can also reduce the ongoing costs of a project by minimising the amount of information being collected or used where this is possible, and devising more straightforward processes for staff.

More generally, consistent use of PIAs will increase the awareness of privacy and data protection issues within an organisation and ensure that all relevant staff involved in designing projects think about privacy at its' earliest stages.

Examples of where a PIA would be appropriate

- A new IT system for storing and accessing personal data.

- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.
- Cloud hosted applications
- The collection of new data on an existing system

A PIA should be used on specific projects and to be effective it should be applied at a time when it is possible to have an impact on the project. This means that PIAs are more likely to be of use when applied to new projects or revisions of existing projects. Procurement practices and procedures are key to the success of this procedure and will be adapted accordingly.

The Council must identify the need for a PIA at an early stage and build this into project management or other business processes.

The Client Department (Commissioner) will be responsible for carrying out the PIA and for completing the necessary templates.

7. PIA Procedure

The format for an initial PIA is at Appendix 2 at **Annex A.**

This review form is based on the Data Protection Principles set out in GDPR.

In the event that a full PIA is deemed appropriate/necessary the format for this is at Appendix 2 at **Annex B**

The links between the PIA and GDPR are set out in Appendix 2 at **Annex C**

It is important, especially in larger projects, to consult with external stakeholders (including where appropriate reviewing data sharing agreements) so that affected parties are involved in the process.

Once the PIA process has been completed consideration should be given as to how the mitigation of risks identified should be incorporated into any Project Plan and also as to whether risks should be included in Departmental Risk Registers.

The completed PIA should be signed off by the senior responsible officer for the project or process in the relevant Department. It should also be logged in the relevant folder in EDRM. PIAs

If any risk is found to be high (16 or over) then this should be signed off by a Service director or equivalent. In cases of very high risk it may be necessary to consider referral to the ICO. The DPO should be consulted in relation to any proposed reference to the ICO – see below.

8. Monitoring

The screening questionnaire responses and/or completed PIA should be submitted to IGG for monitoring purposes. The presumption is that completed PIAs will be published via the Council's website unless there are issues e.g. commercial confidentially that make this inappropriate.

The IGG will also monitor implementation of actions identified in PIAs and scrutinise implementation of PIA mitigation on a twelve monthly basis by receiving exception reports.

This procedure will be reviewed in September 2018.

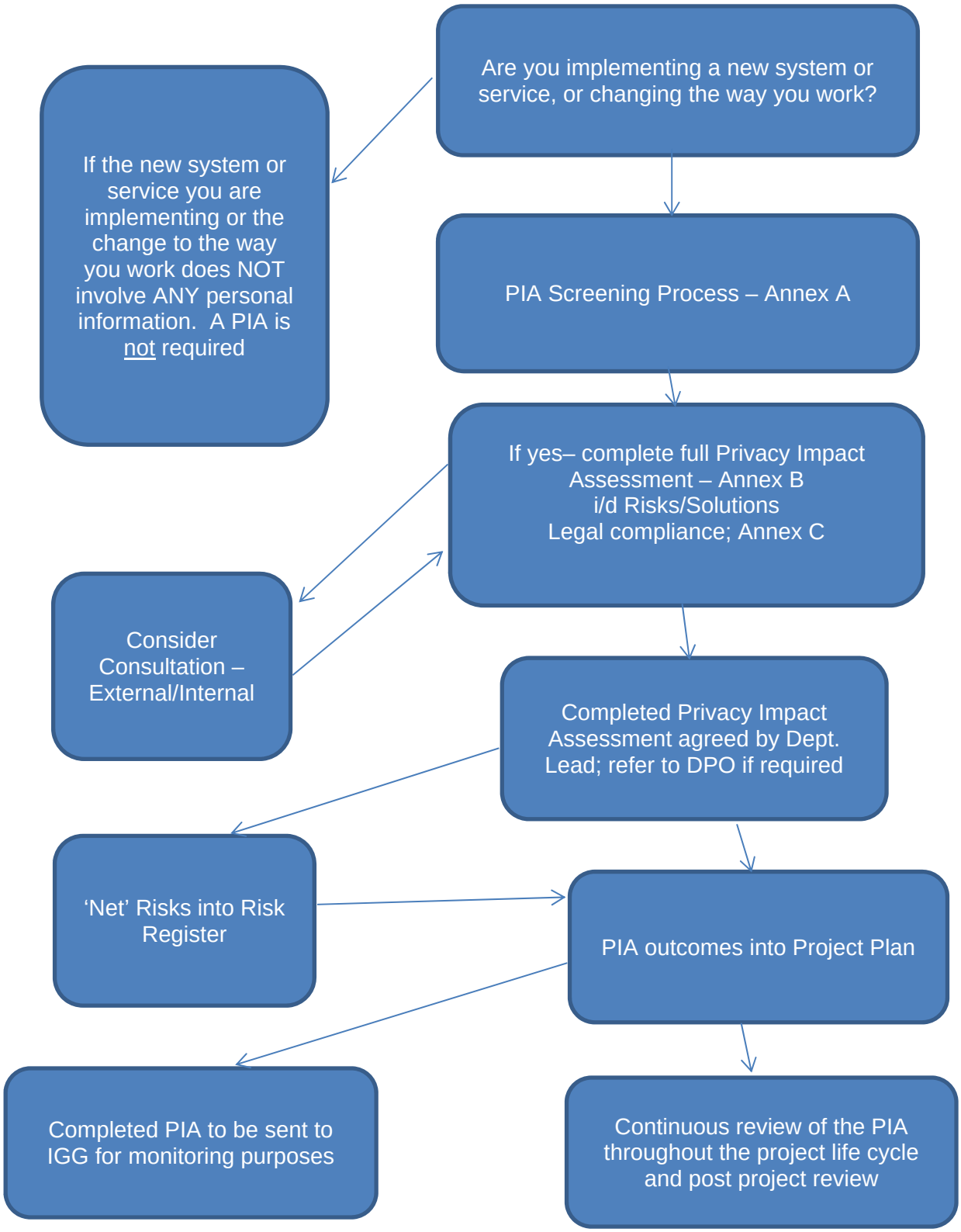
9. ICO role

If the assessment process suggests that the risk to privacy is very high even after any mitigation is applied then it may be necessary to refer the completed PIA to the ICO and consult with them. The ICO have indicated it will take between 8 and 14 weeks for a written response.

The DPO should be consulted **before** any PIA is referred to the ICO under this provision.

Appendix 1

PRIVACY IMPACT ASSESSMENT PROCESS CHART



Appendix 2

Annex A - PIA Screening Questions

Question	Y/N	Additional Comments (please give reasons for either a 'yes' or' no 'answer here
Is there a requirement under GDPR to carry out a PIA? See section 7 above. NB if there is a legal requirement to carry out a PIA there is no requirement to complete the remaining questions.		
Will the project involve the collection of new information about individuals?		
Will the project compel individuals to provide information about themselves?		
Will information about individuals be disclosed to third party organisations or people?		
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.		
Will the project result in you making decisions or taking action against		

individuals in ways that can have a significant impact on them?		
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union information, biometric data, health or information concerning an individual's sex life or sexual orientation or other information that people would consider to be private.		
Will the project require you to contact individuals in ways that they may find intrusive?		
Will the data be held in relation to children or vulnerable adults?		

Annex B Step 1 – Requirement for PIA – issues to be addressed

To Include:

- Project Aim and Objectives
- Benefits to the organisation, to individuals and to other parties of personal data
- Links to any relevant project documentation
- Summary of Identified Need for PIA (can draw on answers to the screening questions).

Annex B Step 2 – Information Flows/Nature of processing

To Include:

- Description of collection, use, retention and deletion of personal data- is any sharing of data involved?
- Explanation of data flows – diagram or description detailing: controllers and processors, storage location and storage method, personal data fields collected, individual/team/organisational access to personal data(audit trail), security measures for storage and transfer of data
- Number of individuals likely to be affected by the project-do they include children or other vulnerable groups?
- A flow diagram is likely to be helpful here.
- Does the data include special category or criminal offence data?

Annex B Step 2 – Consultation Requirements

Identify whether internal and/or external consultation is required to address privacy risks

- Stakeholders to be consulted
- Method of consultation

Part B Steps 3 to 4 – Identify Privacy Risks, Solutions and Approval

Privacy Risk	Risk to Individuals & organisation	Risk initial score	Action Identified	Target Score (after applying actions)	Risk Control Plan (Treat/Control/Tolerate/Accept/Terminate/Transfer)	Evaluation: is the final impact on individuals and the organisation after implementing each solution a justified, compliant and proportionate response to the aims of the project?	Approved By

Step four: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns
Date of consideration by IGG

Annex C

Linking the PIA to the GDPR principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the GDPR or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully

There must be lawful basis for processing the personal data as follows;

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

- Have you identified the purpose of the project and which lawful basis applies?
- Is the processing of the data necessary in terms of GDPR?
- How will you tell individuals about the use of their personal data?
- Do you need to amend your privacy notices?
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If special categories of personal data have been identified have the requirements of GDPR been met?

As the Council subject to the Human Rights Act, you also will where privacy risk are especially high need to consider:

- Will your actions interfere with the right to privacy under Article 8?
- Have you identified the social need and aims of the project?
- Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

Does your Privacy Notice cover all potential users?

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under GDPR.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

Will the system allow compliance with individual rights under GDPR, in particular the right to be informed, the right to rectification and the right to ensure (right to be forgotten).

If the project involves marketing, have you got a procedure for individuals to opt in to their information being used for that purpose?

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?

If you will be making transfers, how will you ensure that the data is adequately protected?