DERBYSHIRE
County Council

Information Security Document

Privacy Impact Assessment Guidance

Version 5.0

Version History			
Version	**Date**	**Detail**	**Author**
1.0	26/11/2017	First Draft for consideration by IGG	Simon Hobbs
2.0	08/01/2018	Approved by Information Governance Group.	Simon Hobbs
3.0	07/02/2018	Impact Assessment table added.	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	Clarifications re department leads following workshops and GDPR.	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

Note

This Guidance Document should be read in conjunction with the Privacy Impact Assessment Procedures.

Introduction

A Privacy Impact Assessment (PIA), also known as Data Protection Assessment (DPIA) is a process which helps assess privacy risks to individuals in the collection, use and disclosure of personal information.

The PIA template is a practical tool to help identify and address the data protection and privacy concerns at the design and development stage of a project, building data protection compliance in from the outset rather than bolting it on as an afterthought.

This document details the process for conducting a Privacy Impact Assessment (PIA) through a project lifecycle to ensure that, where necessary, personal and sensitive information requirements are complied with and risks are identified and mitigated. A PIA should be carried out whenever there is a change that is likely to involve a new use or significantly change the way in which personal data is handled, for example a redesign of an existing process or service, or a new process or information asset is being introduced or when changes are being made to a data sharing agreement. There will be a legal requirement from May 2018 to carry out a PIA where any of the conditions set out in Paragraph 7 of the Procedure are met.

Building into Project Plans

The flowchart at Appendix 1 shows how PIAs should operate within projects

Completion of a PIA should be built into the organisational business approval and procurement processes. Any systems which do not identify individuals in any way do not require a PIA to be completed. However, it is important to understand that what may appear to be “anonymised” data, could in fact be identifiable when used with other information, so anonymised data should be considered very carefully before any decision is made that it will not identify individuals. Advice may be sought from the Council‘s Data Protection Officer as to whether a PIA needs to be completed

Responsibility for Conducting a PIA

Any department which is introducing a new or revised service or changes to a new system, process or information asset is responsible for ensuring the completion of a PIA. The project manager will assist with this process.

At the start of the design phase of any new service, process, purchase of, implementation of an information asset etc. consideration should be given to the need and procedures for completing the PIA. Privacy Impact Assessment outcomes should be routinely reported back to the organisation and issues raised through the project/programme board and included in the Departmental Risk Register as appropriate.

Where significant risks are identified these should be aired, in the first instance, with the DPO who should discuss with the Caldicott Guardian (CG)/Senior Information Risk Owner (SIRO) as necessary.

The Three Stages of a PIA

Stage A - The initial screening questions

This document is to be completed by the Departmental lead responsible for delivering the proposed change. The purpose of the screening questions is to ensure that a further PIA assessment is required and ensure that the investment in the organisation is proportionate to the risks involved. If a response to any of the questions is “yes” then a Privacy Impact Assessment should be considered.

Stage B – Privacy Impact Assessment

This document is to be completed by the Departmental lead responsible for delivering the proposed system/application who will seek advice from the DPO where necessary.

There are 4 Steps to complete within Stage B:

Step 1: Outline Requirement
To Include:

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

Step 2: Information Flows
To Include:

- Description of collection, use, retention and deletion of personal data
- 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

Step 3: Consultation Requirements
Identify whether internal and/or external consultation is required to address privacy risks

- Stakeholders to be consulted
- Method of consultation

Step 4: Identify Privacy Risks, Solutions and Approval
To identify the information risks and describe the mitigation that will need to be put in place to minimise the risk and impact on the Council.

Privacy Risk: Identify and detail the risk and those affected

Compliance Risk: Identify the Compliance Risk from Annex C

Initial Score: Calculate the total score of the risk without any action plans to reduce the level of risk by multiplying the level of score from the Impact Assessment Criteria table with the score from the Likelihood Assessment Criteria table. This is to provide an indication of the worst case scenario.

Impact Assessment Criteria	
Level	**Description**
5	Catastrophic
4	Major
3	Moderate
2	Minor
1	Insignificant

Likelihood Assessment Criteria	
Level	**Description**
5	Expected (monthly)
4	Likely (annually)
3	Possible (1 incident in 2 years)
2	Unlikely (1 incident in 5 years)
1	Rare (1 Incident in 10 years or above)

IE if the impact is at level 5 and the likelihood is level 3: the score would be 5x3=15

Action Plan:
Detail the plans to reduce the risk or what controls are to be put in place.

Target Score
Using the scoring formula in the tables above, calculate the score once controls are in place.

Risk Control Plan: insert risk control definition as appropriate

Risk Control Definitions	
Take the Opportunity	Accept the risk and turn it into a positive opportunity or benefit
Treat/Control	Actions required to mitigate the likelihood and/or impact
Tolerate/Accept	No action - risk within tolerance or accept - Understand and live with the risk.
Terminate	Cease or avoid the risk
Transfer	Transfer to potential third party via contract or bond or insurance etc

Evaluation:
Is the final impact on individuals justified, compliant and proportionate to the aims of the project?

Approved By:
If the Target score (i.e. after mitigation is applied) is over 16, this must be signed off by a Senior Manager at Service Director level or equivalent.

In certain circumstances (where there is a very high unmitigated risk) it may be necessary to consult with the ICO itself. Please take advice from the Council DPO if you think this may apply to your project.

Consent
Is any data special category data as defined in the GDPR involved? If so consent of the data subject may be required.

Step 5: Integrate the PIA outcomes back in to the project plan:
Who is responsible for integrating the PIA outcomes back in to 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?

Stage C Compliance

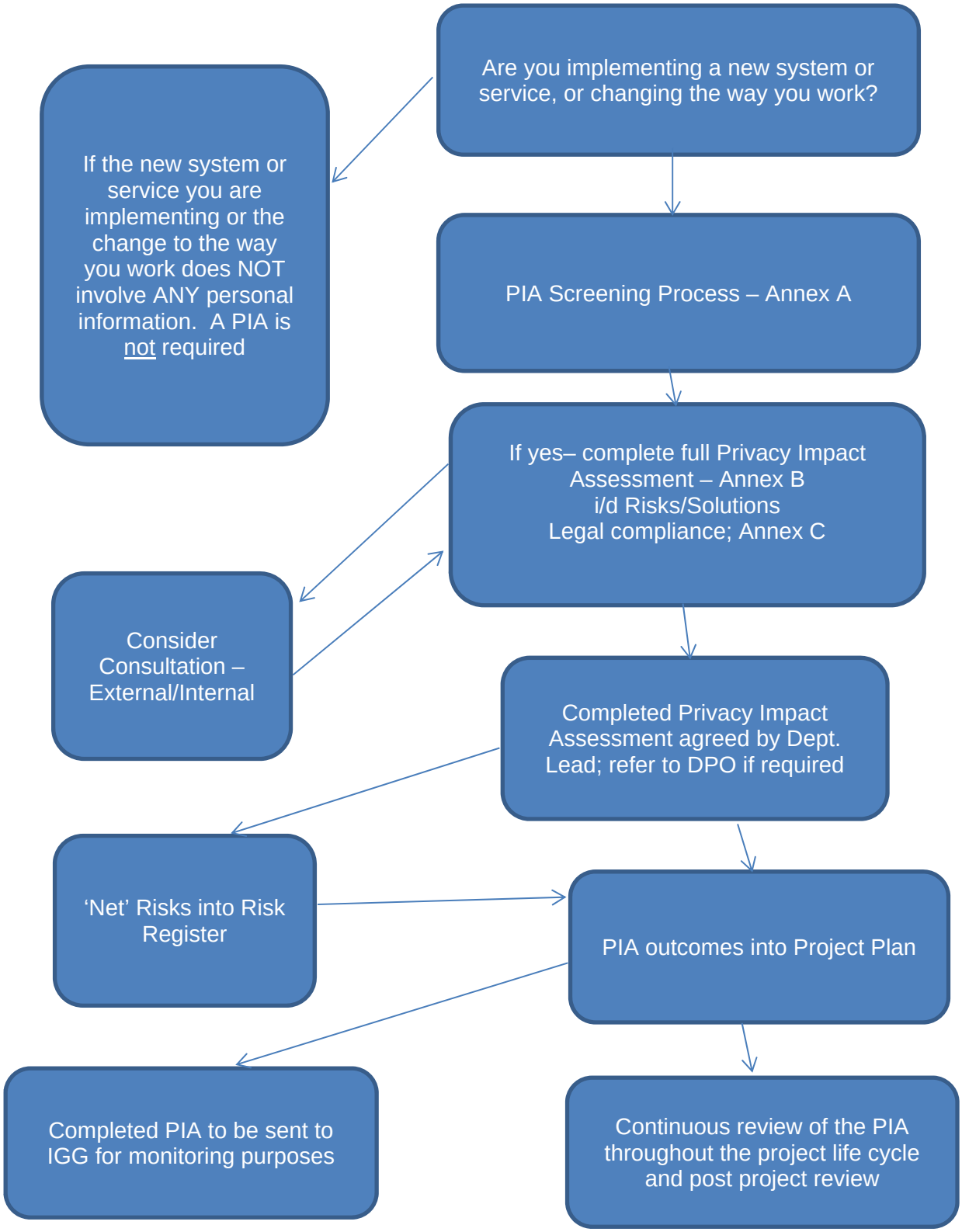
Compliance Assessment – see Annex C

The PIA will be assessed against the compliance checklist which includes the GDPR, Common Law Duty of Confidentiality and the Human Rights Act. Any risks will be noted and solutions put forward, these will be agreed by the project lead and signed off by a senior manager in the Department (for a project the senior responsible officer). Legal advice should be sought if any compliance issues are identified.

The PIA is a dynamic document and should be reviewed regularly throughout the project lifecycle.

The responses to screening questions and/or the completed PIA will, for the time being, be forwarded to IGG for monitoring purposes

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy.

Appendix 1: Flowchart

PRIVACY IMPACT ASSESSMENT PROCESS CHART