PRIVACY IMPACT ASSESSMENT POLICY & PROCEDURE (LA Adopted)

Date this policy was formally reviewed and agreed by the Full Governing Body:	
Signed on behalf of the Governing Body by:	Jeanne Pratt
Signature:	
Date:	24th May 2018
Date of next review:	Summer Term 2021

Introduction

Privacy Impact Assessments (PIA) are an integral part of taking a 'privacy by design' approach. A PIA is a process which minimises the privacy risks of new projects or work activities by considering the impact that the proposed project or activities will have on the individuals involved to ensure that potential problems are identified at the outset and addressed.

This guidance is based on comprehensive guidance produced by the Information Commissioner's Office which can be accessed at; https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

When is a PIA required?

You must carry out a PIA whenever you are implementing or making a change to a process or system, project or work activity that could have an impact on the privacy of individuals.

Stages of a PIA

Stage 1 - The initial screening questions

This section is to be completed by the service manager or project lead responsible for delivering the proposed change. The purpose of the screening questions is to assess whether a further PIA assessment is required and ensure that the investment in the Authority is proportionate to the risks involved**.**

- If the answers to the questions are no **-** The screening process has not identified any PIA concerns and the process is complete
- If response to any of the questions is "yes" then an initial Privacy Impact Assessment must be undertaken

It is important to get this stage right. If we are challenged by the Information Commissioner we have to be able to defend the decision about why we did or did not undertake a PIA..

Stage 2 – Privacy Impact Assessment

The responses to the screening questions will give an indication as to the appropriate scale of the PIA. In some cases, the answers to the screening questions may not be known and the process will need to be re-visited when more information comes to light.

The PIA (Appendix B) must be completed by the service manager or project lead responsible for delivering the proposed change. A copy of the completed form must be sent to the Data Protection Officer in order to provide further guidance if necessary. There are three possible outcomes to the initial PIA:

- The initial PIA is incomplete and will have to be repeated or further information obtained.
- The initial PIA is complete and no privacy risks have been identified.
- The initial PIA has identified privacy risk.

Stage 3 – Identifying Compliance Risks

Identifying compliance risks (Appendix C) will be necessary where there are any significant IG risks identified. The checklist reviews the Data Protection Principles in order for each to be considered and must be completed by the project lead. A copy of the completed form must be sent to the DPO in order to provide further guidance if necessary and any risks may then be highlighted and escalated to the Senior Information Risk Owner (SIRO).

An action plan must be developed by the project lead, on how the risks will be mitigated. This will include identified issues, associated actions, related roles and responsibilities and timescales.

Measures to reduce the risk

It is important to remember that the aim of a PIA is not to completely eliminate the impact on privacy. The purpose of the PIA is to reduce the impact to an acceptable level while still allowing a useful project to be implemented.

Examples of measures:

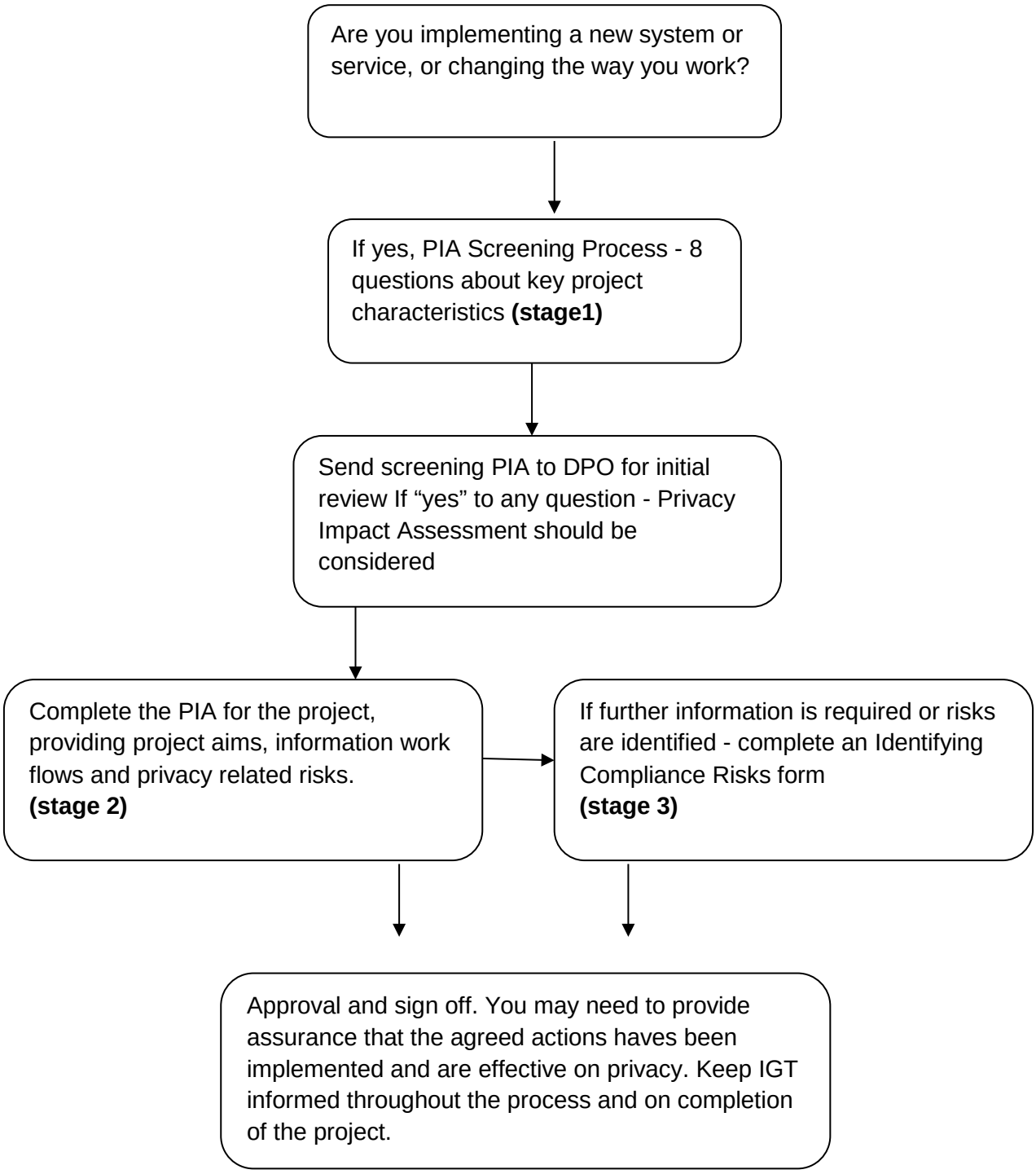
- Obtaining the data subject's consent;
- Deciding not to collect or store particular types of information;
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information;
- Implementing appropriate technological and organisational security measures;
- Ensuring that staff are properly trained and are aware of potential privacy risks;
- Developing ways to safely anonymise the information, using the Authority's anonymisation guidelines, when it is possible to do so;
- Producing guidance for staff on how to use new systems and how to share data if appropriate;
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests;
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the Authority for assistance if necessary;
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an Authority's behalf;
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Integrating the PIA outcomes back into the project plan

The PIA findings and actions should be integrated with the project plan. The person responsible for the PIA and the overall project should ensure that the steps recommended are implemented and return to the PIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.

If the PIA generates actions which will continue after the assessment has finished, the person responsible should ensure that these are monitored and that all lessons learnt from the PIA are recorded for future projects.

Flowchart


Are you implementing a new system or service, or changing the way you work?
If yes, PIA Screening Process - 8 questions about key project characteristics **(stage1)**
Send screening PIA to DPO for initial review If “yes” to any question - Privacy Impact Assessment should be considered
Complete the PIA for the project, providing project aims, information work flows and privacy related risks. **(stage 2)**
If further information is required or risks are identified - complete an Identifying Compliance Risks form **(stage 3)**
Approval and sign off. You may need to provide assurance that the agreed actions haves been implemented and are effective on privacy. Keep IGT informed throughout the process and on completion of the project.

Appendix A

Privacy Impact Assessment (PIA) Initial Screening Form

Project name:		**Date:**
Brief project outline:		
Project Lead Officer:		

PIA Screening Questions

These questions are intended to help the Authority decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise.

Once completed please return to the Information Governance Team for review:

Question	Yes/No (√)		Notes
Will the project involve the collection of new information about individuals?	**Y**	**N**	
Will the project compel individuals to provide information about themselves?	**Y**	**N**	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	**Y**	**N**	
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	**Y**	**N**	
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	**Y**	**N**	
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	**Y**	**N**	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	**Y**	**N**	
Will the project require you to contact individuals in ways which they may find intrusive?	**Y**	**N**	

DPO Feedback/Decision:

IGT Use only:
Date: **Officer:**

Appendix B

Privacy Impact Assessment (PIA)

Project name:		**Date:**
Brief project outline:		
Project Lead Officer:		

Step 1: Identify the need for a PIA:

Explain what the project aims to achieve, what the benefits will be to the Authority, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a PIA was identified (this can draw on your answers to the PIA Initial Screening Questions)

Step 2: Describe the information flows

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Step 3: Describe the information flows

Consultation requirements - Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the PIA process.

Step 4: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. (Please refer to the 'PIA – Identifying Compliance Risks' to help identify the DPA related compliance risks):

Privacy issue	Risk to individuals	Compliance risk	Associated organisation/corporate risk

Step 5: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems):

Risk	Solution(s)	**Result:** is the risk eliminated, reduced or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step 6: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step 7: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes 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 which may arise in the future?

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

Appendix C

Privacy Impact Assessments (PIA) - Identifying compliance risks

Project name:		**Date:**
Brief project outline:		
Project Lead Officer:		

Answering the below questions during the PIA process will help to identify where there is a risk that the project or activity will fail to comply with the Data Protection Act (DPA) or other relevant legislation, for example the Human Rights Act:

Principles of the Data Protection Act 1998	Question	Answer
Principle 1 - Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: **a) at least one of the conditions in Schedule 2 of the DPA is met and** **b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 of the DPA is also met.**	Have you identified the purpose of the project? How will individuals be told about the use of their personal data? Do you need to amend your privacy notices? Have you established which conditions for processing apply? 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? As an Authority we are subject to the Human Rights Act, we therefore also need to consider: whether our 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 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 potential new purposes been identified as the scope of the project expands?	
Principle 3 - Personal data shall be adequate, relevant and not excessive in relation	Is the information you are using of good enough quality for the purposes it is used for?	

to the purpose or purposes for which they are processed.	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 processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.	What retention periods are suitable for the personal data you will be processing? Are you procuring software/systems which 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 this Act.	Will the systems you are putting in place allow you to respond to subject access requests more easily? If the project involves marketing, have you got a procedure for individuals to opt out of 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?	