Privacy Impact Assessment (PIA)

Privacy Impact Assessments (PIA) are carried out as part of the Integrated Impact Assessment on all council significant decisions and as part of the IT project process, if personal information is involved and there are risks to the privacy of individuals. The PIA will consider the risks of complying with legislation such as the DPA and document work required to resolve any design issues, including the alternatives considered and why the option chosen was selected.

The size of the PIA should reflect the scale of the project or change and the following questions should be considered when deciding whether or not to carry out a PIA:

No	Question	Response
1	Will the project/decision involve the collection of new information about individuals?	Yes
2	Will the project/decision require individuals to provide information about themselves?	Yes
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Yes
4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Yes
5	Does the project/decision involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	No
6	Will the project / decision result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	No
7	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 private.	Yes
8	Will the project/decision require you to contact individuals in ways that they may find intrusive?	No

The following PIA Template should be used to carry out the assessment and record the results. Further information to help determine whether the project/decision will comply with the DPA is also included.

Privacy Impact Assessment Template

Step One - Identify the need for a PIA
(Summarise why a PIA is required)
Collecting and processing personal information. The personal information being collected will include sensitive personal information for which the respondent will have clear privacy expectations.

Overall assessment of all consultation activity.

Individual high profile consultation will review this PIP and amend where appropriate.

Step Two - Describe the Information Flows
(Describe how personal information will be collected, used and deleted and how many individuals are likely to be affected)
Various options have been explored and processes mapped for each flow.

Step Three - Consultation Requirements
(Explain who should be consulted internally and externally to ensure that all privacy risks have been explored and how this will take place)

Information security and assurance board
Communications and marketing team
Service requesting consultation
Partner organisations involved in the consultation
Survey testing forum – made up of employees of partner organisations
Services/location involved in collection of data
Respondents piloting data collection methods

Step Four – Identify the Privacy Related Risks
(Identify the key privacy risks and any associated compliance or corporate risks – larger projects might record this information on a formal risk register). See Appendix D for information that will help to determine if there is a risk of not complying with the Data Protection Act)

Privacy Issue	Risk to Individuals	Compliance Risk	Associated Organisation / Corporate Risk
No lawful purpose for survey or particular question.	Unnecessary intrusion of privacy	Non-compliance with the DPA and HRA	Consultation not lawful. Potential complaint and reputational damage. ICO fine/enforcement.
Respondents not fully informed of why their data is collected.	Information not used for the purpose stated. Not consented to processing.	Non-compliance with the DPA and HRA	Consultation not lawful. Potential complaint and reputational damage. ICO fine/enforcement.
Data is accessible to unauthorised individuals.	Unwarranted intrusion causing potential harm and distress.	Non-compliance with the DPA and HRA	Potential complaint and reputational damage. ICO fine/enforcement.
No reason for survey or particular question.	Unnecessary intrusion of privacy	Non-compliance with the DPA and HRA	Consultation not lawful. Potential complaint and reputational damage. ICO fine/enforcement.
Collection method is intrusive	Unwarranted intrusion causing potential harm and distress.	Non-compliance with the DPA, HRA and PECR	Potential complaint and reputational damage. ICO fine/enforcement.
Insufficient or inadequate information	Unwarranted intrusion causing potential harm	Non-compliance with the DPA and HRA	Potential complaint and reputational damage.

collected to meet the requirements of the consultation.	and distress.		Unnecessary cost to re-run consultation.
Data collected is either inaccurate or out-of-date.	None	None	Misinformed decision making, unnecessary costs.
Personal identifiable information is kept longer than necessary.	Unwarranted intrusion causing potential harm and distress.	Non-compliance with the DPA and HRA	Potential complaint and reputational damage. ICO fine/enforcement.
Controls are not in place to keep data protected and secure.	Unwarranted intrusion causing potential harm and distress.	Non-compliance with the DPA and HRA	Potential complaint and reputational damage. ICO fine/enforcement.
Step Five – Identify Privacy Solutions (Describe the actions you could take to reduce risks)			
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 & proportionate response to the aims of the project?
No lawful purpose for survey or particular question.	Follow good practice guidelines which include identifying the lawful purpose for the consultation and reviewing of all questions.	Reduced to an acceptable level.	Yes
Respondents not fully informed of why their data is collected.	Clear privacy notice and guidance with the survey provided to respondents.	Eliminated	Yes
Data is accessible to unauthorised individuals.	Secure arrangements in place for the storage and transfer of survey data, preventing unauthorised access.	Reduced	Yes
No reason for survey or particular question.	Follow good practice guidelines which include identifying the lawful purpose for the consultation and reviewing of all questions.	Reduced to an acceptable level.	Yes
Collection method is intrusive	Follow good practice guidelines in the undertaking of consultations. Any new collection methods will be fully evaluated and reviewed.	Reduced to an acceptable level.	Yes
Insufficient or inadequate information collected to meet the requirements of the consultation.	Follow good practice guidelines which include identifying the lawful purpose for the consultation and reviewing of all	Reduced to an acceptable level.	Yes

	questions.		
Data collected is either inaccurate or out-of-date.	Follow good practice guidelines which include the reviewing of all questions.	Reduced to an acceptable level.	Yes
Personal identifiable information is kept longer than necessary.	Retention schedules have been established for consultation activities which are actively managed and enforced.	Reduced to an acceptable level	Yes
Controls are not in place to keep data protected and secure.	Secure arrangements in place for the storage and transfer of survey data, preventing unauthorised access. Data is backed up via a download from the software where it is held. Data is also retained at an aggregated and anonymised level.	Reduced	Yes
Step Six – Sign off and Record the PIA Outcomes (Who has approved the privacy risks involved in the project and what solutions need to be implemented?)			

Step Seven – Integrate the PIA Outcomes back into the Project Plan
(Who is responsible for integrating the PIA outcomes back into the project plan & 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

Linking the Privacy Impact Assessment to the Data Protection 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 DPA or other relevant legislation, for example the Human Rights Act.

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 is met, and
b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?	Yes
How will you tell individuals about the use of their personal data?	PN/in survey
Do you need to amend your privacy notices?	Assessed at each survey
Have you established which conditions for processing apply?	explicit consent
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?	Respondents will complete survey in different formats voluntarily and will be fully informed of the purpose the information is being collected for, how it will be used and who it will be shared with. Details of how to withdraw consent are available on the consultation webpage.
If your organisation is subject to the Human Rights Act, you also need to consider:	
Will your actions interfere with the right to privacy under Article 8?	No
Have you identified the social need and aims of the project?	Yes – To obtain the views of respondents to inform decision making.
Are your actions a proportionate response to the social need?	Yes

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?	Yes
Have you identified potential new purposes as the scope of the project expands?	Aware of it and built

	into established procedures

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?	Data quality is part of the process of setting up the survey
Which personal data could you not use, without compromising the needs of the project?	Established procedures ensure only minimum required information is collected

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?	N/a
How are you ensuring that personal data obtained from individuals or other organisations is accurate?	Postcode data is validated. All other data is the views of the respondent and cannot be validated for accuracy.

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?	3 years has been set for the retention of person identifiable data.
Are you procuring software that will allow you to delete information in line with your retention periods?	Current software (survey monkey and achieve) allows data to be deleted in line with retention schedules. Any procurement of new software would insure data can be deleted in accordance with the retention schedule.

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

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

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?	No

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