

Privacy impact assessment

Step one: Identify the need for a PIA

Explanation of what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties and why a PIA was considered necessary.

The aim of the project is to update the start the process of reviewing and replacing the Scarborough Borough Local Plan. The benefits of this are that the Council has a sound basis for determining planning applications and the directing of housing and other forms of development to appropriate sites.

The need for the PIA was established by screening the proposed project. This confirmed that part of the consultation process will be the submission of personal details (name, address, contact details) in addition to any comments received. Whilst many of the comments are likely to be from organisations there is will be considerable involvement from communities and individuals within the Borough.

Step two: Describe the information flows

Description of the collection, use and deletion of personal. How many individuals are likely to be affected by the project?

The number of individuals affected by the project is unknown as this will depend on the actual response rate.

The information collected in this instance will be both organisations and individual's comments on the proposed review of the Local Plan. This will be used to determine what the main issues and options associated with the Plan review are likely to be prior to taking the review forward and releasing further draft and submission versions of the document. Any comments must be duly made and this involves the submission of a person's name and contact details; be that a physical address or email address. The submission of comments cannot be done anonymously as this opens up such processes to abuse and multiple responses from a single or small number of persons which can significantly skew any results of a consultation exercise.

The comments received will be retained for the period of the project and for a further period equivalent to any legal requirements associated with challenges to the document or a judicial review. At the current time the Regulations allow a period of 6 weeks for judicial review from the time of adoption.

Beyond that date the comments collected can be deleted along with any names and addresses unless said respondent has specifically asked to be kept informed of any further policy consultations.

If a person asks for their contact details to be retained for the purposes of future consultation that may be of interest then they will be contacted at future dates to ensure ongoing explicit agreement to remain on the consultee list.

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?

Internal Consultation

GDPR Officer – discussions have previously taken place the relevant officer who has responsibility for GDPR matters corporately on very similar projects who has assisted in identifying potential privacy risks and appropriate mitigation measures for that occasion and future project events.

Planning Manager – has been consulted and is aware of the need to undertake the consultation as well as the fact that measures are being implemented to reduce risk and increase transparency.

Internal system users – those administering the software within the planning service have received appropriate training and have ongoing input into the management of privacy risks. Access by system users is password protected.

External Consultation

Software provider – the provider of the Objective Keystone software (which will host the consultation results) has been previously consulted to ensure that appropriate security and risk

management functions are integrated to ensure compliance with the GDPR. The current software meets the information security standards ISO27018.

In this respect the amount of personal data collected is likely to be minimal (names, address, email). In addition, the nature of the personal data is not considered to be particularly intrusive or of a sensitive nature. It is therefore considered disproportionate to undertake external consultation with these persons.

All consultees will be provided the opportunity to view appropriate information (including a Privacy Notice) about processing activities and purposes prior to submitting a response.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Access to names and addresses including other contact details.	The unauthorised access to data could result in individuals being contacted by non-authorised persons and their address details (including email) being accessed by others.	Non-compliance with DPA	Non-compliance with DPA can lead to fines and reputational damage. Storage of information that is no longer required or useful.

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary

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?
Access to consultees name, address and contact details.	1) The information is stored securely on the Objective software system (ISO 27018 compliant) and where requested deleted after a set period. 2) Ensure only relevant persons in the planning section have access to the data held on the system and ensure that any persons no longer in the employ of the section have their access rights removed immediately. 3) Storing all paper submissions securely and then confidentially destroying all	With the solutions set out the risk is reduced and access to consultee data would have to be through an unauthorised access into the software. Likelihood is considered to be substantially reduced with these measures.	In respect of the data collected in this instance the manner in which it is stored and proposed for disposal (if that is what the respondent requests) is considered satisfactory and proportionate to the aim to update the affordable housing SPD.

paper submitted comments once the set period has expired.
 4) Removal of person's personal data from the software system once the set period has expired if they have not requested to be retained as a future consultee.

Step five: 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
<p>Access to consultees name, address and contact details</p>	<p>The use of secure software as set out under Step 4 and the restricted access to data – only access for Planning Policy staff.</p> <p>Confidentially destroying of paper comments once the set period has expired.</p>	<p><u>Alison Johnson – Audit and Fraud Manager</u></p> <p><u>Wendy Trainor – SIRO Officer</u></p>

	Removal of person's personal data from the software system once the set period has expired if they have not requested to be retained as a future consultee.	
--	---	--

Step six: 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
<ol style="list-style-type: none"> 1. Use the Objective Keystone system for storage of data and comments. 2. Check staff access to software and limit to those within the Planning Policy section. 3. Store any paper submissions securely that contain any personal data for the duration of the 	<ol style="list-style-type: none"> 1. During the consultation event. 2. Prior to the consultation event commencing. 3. During the consultation event for secure storage. Removal of data as soon as possible after the end of any judicial review 	Planning Policy Team for (1, 3) Steve Wilson for (all)

<p>project and confidentially dispose of once the appropriate time has passed (likely to be adoption of SPD plus 3 months).</p> <p>4. Removal of any personal data from Objective Keystone after the aforementioned passing of time if the consultee has not requested to be retained on the consultee list for future consultation purposes.</p>	<p>period or if a judicial review is held once that has concluded.</p> <p>4. As soon as possible after the end of any judicial review period or if a judicial review is held once that has concluded.</p>	
<p>Contact point for future privacy concerns</p>		
<p>Steve Wilson</p>		

Signed off by.... Alison Johnson (Audit and Fraud Manager) Date: 8/7/19