BRENTWOOD BOROUGH COUNCIL

Privacy Impact Assessments Policy

1st Draft

Title:	Privacy Impact Assessments Policy
Purpose:	To ensure we assess and manage risk appropriately around personal data when adopting new or amended systems, contracts and processes
Owner:	Data Protection Officer
Approved by:	Head of Legal Services
Date:	July 2017
Version No:	1.0
Status:	SUBJECT TO COMMITTEE APPROVAL
Review Frequency:	Annually or when changes made to relevant Information Governance law
Next review date:	As above
Meta Compliance	IT to ensure policy subject to this

Introduction

This policy defines the Privacy Impact Assessments Policy and is part of the Information Governance suite of policies currently under review. If you require advice and assistance around any Information Governance matters (including for example Data Protection, data security and FOI requests) please contact the council's Data Protection Officer (DPO). Further information and resources including training and other online support are available on the council's intranet.

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must I do?

1. If you are managing any initiative to create a new process or contract or amend an existing process or contract which involves the use of personal data or business sensitive data, you must contact the Data Protection Officer (DPO) to begin the Privacy Impact Assessment (PIA) porcess.

2. If you are managing an initiative which requires a PIA, you must begin the PIA process in the planning phase of any project cycle or new contract.

3. PIA's must be approved* before any activity being considered under the PIA is implemented.

4. The owner of the process being considered under a PIA is responsible for drafting the PIA.

5. *PIA's must be reviewed and a decision on approval made by the Data Protection Officer.

6. The Data Protection Officer must keep a central record of PIA's carried out by Services; the PIA's will identify risks and mitigations and approvals.

7. The Data Protection Officer will monitor performance against this policy and report to the Senior Information Risk Officer on areas for improvement.

8. The Data Protection Officer will review PIA's to ensure that the requirements identified have been fully implemented.

Why must I do it?

1. To comply with the Information Commissioner's Code of Practice supporting compliance with the Data Protection Act, which may be viewed at:

https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

This document includes a PIA template for you to complete.

2. A PIA may arrive at an outcome that the proposals in an initiative are not appropriate due to the degree of risk to the Council of breaching the Data Protection Act. In such instances, the Data Protection Officer will suggest possible alternatives, but may refuse to approve the proposal. If work has already begun on implementing the proposal and contractual arrangements have been entered into before being approved under a PIA, this would represent a breach of this policy. This may result in the discontinuance of work already commenced and present BBC with legal, contractual and financial consequences.

3. The approval of a PIA is the authorisation that BBC is satisfied that ht risks of the proposal are acceptable. This policy is breached by implementing a proposal involving personal data without prior PIA approval, rather than only in the event of something going wrong.

4. The Data Protection Officer can provide advice on what the PIA needs to include but cannot complete the form on your behalf. The review of the PIA needs to be objective.

5. The process needs to be managed by staff trained in the activity and in the requirements of the Data Protection Act.

6. To review and audit the quality of the process. To ensure recommendations in the PIA have been implemented. To assist with future reviews on the same processes.

7. To ensure the process is working and refinements are made to improve performance.

8. To ensure recommendations have been adopted.

How must I do it?

1. If your initiative requires technical IT support, contact the IT manager in the first instance.

2. Once you have identified that personal data will be involved in your proposed project/contract, you should contact the Data Protection Officer for an initial discussion around your proposals and to run through the PIA form.

3. If in doubt about the progress or status of your PIA, contact the Data Protection Officer.

4. Use the Privacy Impact Assessment Form within the Code of Practice document contained in the above-mentioned link.

5. Each PIA will be reviewed by the DPO and proposals reviewed to assess with the process owner risks and consider suggestions for risk mitigation and approval of the PIA once sufficient mitigation has been demonstrated.

6. The DPO will maintain a central record of all PIA's for audit and reference/precedent purposes.

7. Reporting on statistics re: PIA's received, implemented and breaches of policy.

8. DPO to ascertain from the relevant Service Manager that adequate controls are in place.

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you. The Council as well as those individuals affected is also at risk of financial and reputational harm. Currently fines of up to £500,000 may be imposed on Councils for serious data breaches. Please report any actual or potential data breaches or other concerns relating to Information Governance to the Data Protection Officer as soon as possible.

References:

Data Protection Act 1998

Conducting Privacy Impact Assessments Code of Practice (ICO)

Human Rights Act 1998