BRENTWOOD BOROUGH COUNCIL

Privacy Notices Policy

1st Draft

Title:	Privacy Notices Policy
Purpose:	To ensure customers understand how and why their personal data is processed in accordance with the first principle under DPA
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 Notices 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.

What is a Privacy Notice?

Privacy Notices are required whenever it is not obvious to customers how and why we are using their personal information. Privacy Notices must be individually drafted to accurately explain the specific purposes for which we are collecting their personal data and, where applicable, how we may use and share it with others.

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. Whenever we collect personal information about an individual, we must tell them why we are collecting it to assure them that their information is collected and used **fairly in accordance with the first Principle of the Data Protection Act (see further below for list of all DPA Principles).** Personal data is information which could identify a living individual.

2. A Privacy Notice must, as a minimum, tell people who we are, what we are going to do with their information and who it will be shared with.

3. You must consider whether your privacy notice should provide more details such as information about people's rights of access to their data, your arrangements for keeping their data secure and how long it will be kept for.

4. You must review your Privacy Notices annually and where amendments are required to reflect changes to legislation, processes and/or information sharing agreements.

5. Where we collect information on behalf of a third party or vice versa, you must make this clear in the Privacy Notice.

6. If you intend to share the information, this must be included in your Privacy Notice. If the customer has a choice regarding whether the information is shared, this must be communicated and they must be given the opportunity to opt out of sharing. If their is no choice, you should explain in the Privacy Notice why the sharing is necessary.

7. If you would like to send your customers marketing information, including emails to update them on changes to our services, you must first obtain their consent to do this. This should be included in the Privacy Notice.

8. To encourage the public to provide us with their opinion on issues such as where they live or the services we provide, we may run competitions, perhaps attached to surveys. You must include details about how we will make use of their personal data.

9. If you are conducting a survey, you must always consider whether it is possible to collect the information without any personally identifiable information.

10. If we have told someone that their information is to be deleted after a certain period of time, we must ensure that we do this.

11. You must consider that when asking for postcode information that some postcodes can identify individuals' addresses, so this would be treated as personal identifiable information.

Why must I do it? (Note - please see list of the 8 Data Protection Principles further below)

1. This is a legal requirement under Principle 1 of the Data Protection Act 1998.

2. Basic legal requirement where personal data is being collected.

3. The level of detail required in the Notice depends on a number of factors; the more information being gathered, level of sharing and the longer you may want to keep it for dictates the need to explain more. If in doubt, consult the Data Protection Officer.

4. We must ensure that the Privacy Notice remains accurate and relevant to how we actually use the data.

5. The public has a right to know all parties involved in processing their personal data.

6. The public has a right to know all parties involved in processing their personal data.

7. People being able to control the volume and means of being contacted using their personal data is one of the key rights in the Data Protection Act.

8. Because we are collecting personal information, a Privacy Notice will need to be added. People may be more willing to participate if they know how their information will be used, for example, it will not be kept longer than is necessary.

9. Collection of personal data must always be justifiable and proportionate. This protects the privacy of individuals and a Privacy Notice is not always necessary if the information is completely anonymous.

10. Otherwise would be in breach of the Data Protection Act.

11. Particularly in rural areas, a postcode may identify a single property.

How must I do it?

1. This would normally be achieved by providing a statement, known as a Privacy Notice, on the form or paperwork that we are asking customers to complete.

2. A very simple, basic Privacy Notice may read as follows: "Brentwood Borough Council collects your personal information to process your xyz application. This information will not be shared with any other party unless the law requires us to do so". For further guidance on how to draft Privacy Notices, see:

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/how-should-you-write-a-privacy-notice/

3. Consider how you intend to process the data, how it will be used, stored, shared and retained. Consider what concerns customers may have over these issues and what benefits would come from reassuring customers with an explanation, or the risks from failing to provide sufficient explanation to them.

4. A review should look at what has been stated in the current Notice, considering whether anything has materially changed in how the data is being used and managed, and consider whether a change to the Notice is required.

5. The statement would then start as follows: "BBC collects this information on behalf of (third party) who are working in partnership with us for the purposes of (xyz). OR, "(third party) collects this information on behalf of BBC....".

6. If there is no choice available, an example text would be: "Your details, excluding your payment details, will only be shared with (third party) who work in partnership with us for the purposes of (xyz). OR, "We would like to share your information with (third party) so that they can provide further information and advice that may be of benefit to you. If you are happy with us sharing your information for this purose, please tick this box".

7. An example could be: "We would like to contact you in the future to provide updates on xyz. If you would like to receive this information, please tick here".

8. An example could be: "The personal information you have provided will only be used to administer the prize draw and to select a winner at random. We will keep this information for one week after the closing date of the prize draw and will not share your information with anyone".

9. When planning a survey, start with the assumption that no personal data will be gathered. Each element of quality data that relies on personal data being provided should be consdered by balancing the positive outcome for your survey against the level of personal data required to achieve it.

10. In many cases, someone's personal information is not relevant to the information on the survey itself, so if you wish to keep the survey, but not the personal details, make sure these can be removed.

11. Consider whether a full postcode is really necessary. The first 3 or 4 digits of a postcode are considered not to be sufficient to disclose personal data so this would be an acceptable alternative as long as the means of capturing the data make it clear that only part of the postcode is required, or participants are not able to enter more than 4 digits.

The Eight Data Protection Principles

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

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.

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.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

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.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

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.