

BRENTWOOD BOROUGH COUNCIL

# Privacy Notices Policy

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:	March 2018
Version No:	2.0
Status:	APPROVED BY PP&R COMMITTEE 12/3/18
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. If you require advice and assistance around any information governance matters, 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?

A privacy notice is a statement that describes why and how an organisation collects, uses, retains and discloses or shares personal information. The notice should also explain what rights individuals have to control how the council uses their information.

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 there is no choice, you should explain in the Privacy Notice why the sharing is necessary and legally justified.
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, 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 six Data Protection Principles further below)**

1. This is a legal requirement under Chapter 3 of the GDPR

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

3. The level of detail required in the Notice depends on many 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 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/>

and

<https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/>

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 purpose, 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 considered 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 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 if 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 Six Data Protection Principles**

Article 5 of the GDPR requires that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

### **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. Fines of up to €20,000,000 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.