BRENTWOOD BOROUGH COUNCIL

Consent Policy

1st Draft

Title:	Consent Policy
Purpose:	Guidance on obtaining someone's permission to use their personal data
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 Consent 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 must I do?

1. Staff must have respect for privacy and people's right to determine what happens to their personal and sensitive information, except in limited circumstances (please contact the Data Protection Officer (DPO) if you require advice and guidance in such cases.).

2. Individuals have the right to withdraw/withold consent in most circumstances, and this must be respected and recorded appropriately.

3. Consent must be freely given, specific and informed.

4. All employees must ensure they consider the safety and welfare of the individual when making decisions on whether to share information about them.

5. All employees must establish the capacity of the individual's ability to provide consent.

6. When requesting consent, staff must ensure that information is provided in a suitable, accessible format or language for example, by providing large print or Braille versions and also consider the use of accredited interpreters, signers or others with special communication skills.

7. Where it has been established that an individual is unable to give consent (and where there is no existing legal representation) or to communicate a decision, employees must take decision about the use of information by taking into account the individual's best interests and any previously expressed wishes.

8. Where an explicit request by a child that information should not be disclosed to parents or guardians, or indeed to any third party, their decision must be respected except where it puts the child at risk of significant harm, in which case disclosure may take place in the public interest without prior consent.

9. Staff must record the decision to share personal information on an appropriate system which can be readily accessed.

10. Staff must not refuse to share information solely on the grounds that no consent is in place. Each case must be judged on a case by case basis as there will be some circumstances where we can share without the consent of the individual.

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

1. The data subject's consent shall mean any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed (Art 2 Data Protection Directive). All employees must establish the capacity of the individual's ability to provide consent.

2. Individuals in most circumstances have the right to object to information they provided in confidence being disclosed to a third party in a form that identifies them. Where an individual is competent to make such a choice and where the consequences of the choice have been fully explained, the decision should be respected. Careful documentation of the decision making process and the choices made by the individual must be included within their records. If an employee decides to override the refusal to give consent, where possible the individual should be informed of this and the reasoning behind the decision.

3. Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if she/he does not consent. If the consequences of consenting undermine individual's freedom of choice, consent would not be free. Consent by the data subject must be based on an appreciation and understanding of the facts and implications of an action. The individual concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues, such as the nature of the data processed, purpose of the processing, the recipients of possible transfers and the rights of the data subject.

4. The Council acknowledges that obtaining consent is not always possible, or consent may be refused. However, not obtaining consent or the refusal to give consent may not constitute a reason for not sharing information. An individual's information can be disclosed without obtaining consent, if there is an overriding legitimate purpose and it is in the public interest to disclose. All employees must ensure they consider the safety and welfare of the individual when making decisions on whether to share information about them.

5. Seeking consent may be difficult, either because the individual's disabilities or circumstances have prevented them from becoming informed about the likely uses of their information, or because they have a difficulty communicating their decision (be it to consent or object). If an individual is unable to give consent or to communicate a decision, the employee must take decisions about the use of information by taking into account their best interests and any previously expressed wishes, and being informed by the views of relatives or carers as to the likely wishes of the individual. If an individual has made his or her preferences about information disclosures known in advance, this should be respected. Where an individual is incapacitated and unable to consent, information should only be disclosed in their best interests, and then only as much information as is needed to support their care. Each situation must be judged individually and great care taken to avoid breaching confidentiality or creating difficulties for the individual.

6. Seeking consent may be difficult, either because the individual's disabilities or circumstances have prevented them from becoming informed about the likely uses of their information, or because they have a difficulty communicating their decision (be it to consent or object). Extra care must be taken to ensure that information is provided in a suitable, accessible format or language for example, by providing large print or Braille versions.

7. Where an individual is incapacitated and unable to consent, information should only be disclosed in their best interests, and then only as much information as is needed to support their care. Each situation must be judged individually and great care taken to avoid breaching confidentiality or creating difficulties for the individual.

8. The duty of confidentiality owed to a child/young person who lacks capacity is the same as that owed to any other person. Occasionally, children/young people will lack the capacity to consent. An explicit request by a child that information should not be disclosed to parents or guardians, or indeed any third party, must be respected except where it puts the child at risk of siginficant harm, in which case disclosure may take place in the 'public interest' without consent.

9. Employees must gain evidence that consent has been given, either by noting this within a case file, or by including a consent form signed by them.

10. The Council acknowledges that obtaining consent is not always possible or consent may be refused. However, not obtaining consent or the refusal to give consent may not constitute a reason for not sharing information. An individual's information can be disclosed without obtaining consent, if there is an overriding legitimate purpose and it is in the public interest to disclose. All employees must ensure they consider the safety and welfare of the individual when making decisions on whether to share information about them.

How must I do it?

Consult the DPO for further advice and guidance if you are uncertain about how to apply any part of this policy.

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.