BRENTWOOD BOROUGH COUNCIL

Data Consent Policy

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:	February 2018
Version No:	2.0
Status:	APPROVED BY PP&R COMMITTEE
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 document sets out the Council's Data Consent Policy. It covers the processing and sharing of personal data 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.

The GDPR and Consent

The GDPR sets a high standard for consent. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build customer trust and engagement, and enhance the Council's reputation.

The GDPR states that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires individual ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

You must keep clear records to demonstrate consent.

The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw and offer them easy ways to withdraw consent at any time.

Public authorities like Brentwood, employers and other organisations in a position of power may find it more difficult to show valid freely given consent.

You need to review existing consents and your consent mechanisms in your service to check that they meet the GDPR standard. If they do, there is no need to obtain fresh consent.

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/withhold 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.

What if there is no consent?

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 processing or sharing information. An individual's information can be disclosed without obtaining consent, if there is another lawful basis for processing.

The lawful bases for processing are set out in **Article 6 of the GDPR**. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

NB Different criteria apply to **sensitive personal information** (now called "special categories of personal data". This is now defined as data relating to:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

In order to process special category data legally, you must identify **both** a lawful basis under **Article 6 and** a separate condition for processing special category data under **Article 9**. These do not have to be linked. In summary, these are:

(a) explicit consent of the person concerned; or
(b) for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection; or
(c) to protect the vital interests of the data subject or of another natural person; or
(d) processing is carried out with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim (This does not apply to Councils); or
(e) processing relates to personal data which are manifestly made public by the data subject; or
(f) processing is necessary for the establishment, exercise or defence of legal claims; or
(g) processing is necessary for reasons of substantial public interest; or
(h) for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment; or
(i) for reasons of public health; or
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Special Cases

Children

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 significant harm, in which case disclosure may take place in the 'public interest' without consent.

Criminal Offences

The GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in **Article 10**.

To process personal data about criminal convictions or offences, you must have **both** a lawful basis under **Article 6** and either legal authority or official authority for the processing under **Article 10**.

Article 10 also specifies that you can only keep a comprehensive register of criminal convictions if you are doing so under the control of official authority.

How must I do it?

See the checklist at the end of this policy statement and consult the DPO for further advice and guidance if you are uncertain about how to apply any part of it.**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 million 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, in accordance with the Council's Data Breach Policy

CHECKLIST

Asking for consent

☐ We have checked that consent is the most appropriate lawful basis for processing.

☐ We have made the request for consent prominent and separate from our terms and conditions.

☐ We ask people to positively opt in.

☐ We don't use pre-ticked boxes or any other type of default consent.

☐ We use clear, plain language that is easy to understand.

☐ We specify why we want the data and what we're going to do with it.

☐ We give individual (‘granular’) options to consent separately to different purposes and types of processing.

☐ We name organisations and any third-party controllers who will be relying on the consent.

☐ We tell individuals they can withdraw their consent.

☐ We ensure that individuals can refuse to consent without detriment.

☐ We avoid making consent a precondition of a service.

☐ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

Recording consent

☐ We keep a record of when and how we got consent from the individual.

☐ We keep a record of exactly what they were told at the time.

Managing consent

☐ We regularly review consents to check that the relationship, the processing and the purposes have not changed.

☐ We have processes in place to refresh consent at appropriate intervals, including any parental consents.

☐ We consider using privacy dashboards or other preference-management tools as a matter of good practice.

☐ We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.

☐ We act on withdrawals of consent as soon as we can.

☐ We don’t penalise individuals who wish to withdraw consent.