Guidance for obtaining consent for processing personal information

1. Processing Powers

The Data Protection Legislation (the Legislation) and the General Data Protection Regulations (GDPR) govern the means by which the personal information of individuals can be collected and processed by Data Controllers (people or organisations that hold and control the processing of details of living individuals).

As a data controller, Harlow Council must adhere to the legal requirements for processing. There are two approaches to processing that the Council can use; the first being the statutory powers available to the Council as a local authority meaning that consent is not required for processing; the second being relying on consent of individuals.

Failure to comply with these legal requirements could have severe consequences for the Council such as:

- Reputational damage leading to an increase in public distrust and the possibility of a reduction in the level of public engagement.
- The risk of facing the highest tier of administrative fines under the GDPR of up to €20 million or 4% of worldwide annual turnover, whichever is the higher.

1. Relying on Statutory powers for processing

- You can be clear with individuals regarding the powers by which you can legally process their information and the reasons why, without relying on their consent.
- You are not prohibited from processing personal data where you have lawful authority to do so.

- Reliance on statutory powers must be specific – it is not enough to state that the Council can legally process personal data without consent.
- You must be able to prove that the processing is necessary to discharge a public function and is not excessive.
- Reliance on statutory powers cannot be used to obtain information and then be used as a 'blanket' provision for further processing – if you are processing personal data for a purpose different from that stated when the information was obtained, you will be ***unfairly and unreasonably*** processing personal information.

2. Relying on Consent for processing

- By obtaining the consent of individuals for certain types of processing, the Council's risk of unfair and unreasonable processing is reduced**.**

- Obtaining consent allows for broader processing than reliance on a statutory basis for processing which is more limited.

- It is likely that in a number of circumstances, the Council would like to process data beyond the purpose for which it was originally envisaged, but where it has relied on statutory powers, it does not have the authority to do so without the consent of the individual. It would be unproductive and inefficient for the Council to seek individual consent every time this occurred. Therefore, consent to specific processing types should be requested at the point that the personal information is obtained.

- Obtaining consent can build on the Council's reputation by building public trust by being transparent and accountable in regards to how the public's data is held and used. This could enhance levels of public engagement and the Council's relationship with the public generally.

- Consent can be withdrawn at any time and the Council must then immediately stop processing the personal information.

- Individuals have stronger rights in regards to how their information is processed.

When you obtain personal information from individuals you will need to consider why the information is necessary and how the Council intends to process the information (including how the personal information is shared internally between departments). This information will need to be stated within the privacy notice provided to individuals at the point that the Council is obtaining their personal information (more information on privacy notices can be found in the Council's 'Guidance for drafting Privacy Notices').

In most circumstances, by considering how the information will be processed, it will become clear that the statutory basis is not broad enough to satisfy the Council's needs, and reliance solely on this would increase the Council's risk of processing personal information unfairly and unreasonably, thereby breaching the Legislation and the GDPR.

Therefore your approach when obtaining personal information should be to seek consent of the individual where you may wish to process their information beyond the purpose of discharging the specific public function that you are relying on.

2. Obtaining valid consent

The GDPR sets a high standard for consent and specifies the necessary requirements to form valid consent. Consent must be:

a) Freely given

Individuals must have the genuine and ongoing choice and control over how the Council uses their data.

This means that where the Council intends to process an individual's data without consent – under a statutory power – consent should not be sought for this particular processing as the individual does not really have a choice. Asking for consent is misleading and unfair on the individual.

Consent should be clear and distinct – it must be separable from other terms and conditions as well as from other consent options for different types of processing to enable it to be refused and/or withdrawn at any time without detriment to the individual.

b) Specific and Informed

In order for consent to be valid, individuals must be provided with the following information:

- The identity of the Data Controller as well as the name of any third parties who will be relying on consent
- The purposes of the processing and the processing activities. ***Where there are different purposes for processing, separate consents must be obtained. <u>Blanket provisions allowing only for consent to various types of processing for different purposes is prohibited and consent sought in this way will not be valid.</u>***
- The right of the individual to withdraw consent at any time and details of how to do so.

The request for consent must be clear, unambiguous and be in plain language and user-friendly. If the request is vague or too broad it will be invalid.

c) Obtained by affirmative action

It must be obvious that the individual has consented to the processing. There must be a deliberate action of the individual for consent to be valid. A statement requiring confirmation that the terms and conditions have been read is not sufficient.

'Opt-out' boxes and pre-ticked boxes do not constitute valid consent and should not be used. 'Opt-in' boxes may be used but must apply to each separate processing type in order that consent is specific and informed.

d) Documented

- You must keep clear records documenting **each** consent as the GDPR places a duty on data controllers to keep records of processing activities which will be necessary to show compliance. These records regarding consent must specifically document:-Who consented?
- When did they consent?
- How did they consent?
- What were they told?
- Has consent been withdrawn?

Good records will also assist you to monitor and refresh consent as appropriate.

Where consent is withdrawn, it is essential that your department has proper withdrawal procedures in place.
As withdrawal can be at any time, individuals must be able to withdraw consent at any time they choose, on their own initiative, making it as easy to withdraw consent as it was for the individual to provide it.

Ensuring that you have appropriate measures in place for withdrawal of consent and for ensuring your documented consent records are updated is essential.

Where consent is withdrawn no further processing for the purpose for which the consent was relied on can be undertaken. It is essential that officers are aware that consent has been withdrawn and must no longer access or process the personal information for that purpose.

e) Duration of consent

There is no specific time limit for consent, but it is likely to degrade over time. You will need to consider the individual's expectations and the scope of the processing purposes for which the information was obtained. For example:

An individual has completed a form to be a counting assistant for the upcoming local election and has chosen not to consent to their information being held and processed on a database for the purposes of being contacted again for future elections. This individual may be said to have a reasonable expectation that after the local election, their information will only be held and processed for as long as required in regards to audit and tax purposes, after which time their personal information will be securely destroyed.

If the purposes for which you process personal information evolve or change substantially, the original consents may no longer be specific nor informed enough to remain valid consents. Should this situation arise, fresh consents must be sought before the new processing can occur, unless you have another lawful basis for doing so.

Your consent requests should be subject to regular review and you should consider amending them at appropriate intervals. Though no statutory time limit is specified it is good practice to review consents every two years.

Valid consent for processing

Consent will be valid if:	Consent will not be valid if:
✓	✘
It is freely given It is specific and informed including the name of the Data Controller, the purposes of the processing and the types of processing activities It is distinct and separate from other terms and conditions and individuals are provided with the opportunity to consent to each individual processing activity – not one consent for all It obvious that the individual has consented and the affirmative action of the individual is documented The purpose for processing is still fair, reasonable and not excessive so that individuals do not have a reasonable expectation to think that consent should have expired. Any consents provided have been regularly reviewed to ensure that the data is still required and the purpose for processing has not substantially changed making the original consents invalid.	If you have any doubts about whether consent has been provided The individual does not realise they have consented You don't have clear records to demonstrate consent There was no genuine choice on whether to opt-in to different processing types The individual would have been punished for refusing to consent for example not receiving a service or being offered a job. If there is an inequality of bargaining power where the person felt obliged to give consent. The consent was bundled with other terms and conditions The consent request was vague and unclear The consent request used pre-ticked or opt-out boxes The Data Controller was not named The consent request did not contain information regarding an individual's right to withdraw consent Individuals cannot withdraw consent easily The processing purposes for which consent was obtained have substantially changed meaning that the consent request would be unspecific and uninformed for the new processing purposes