Guidance for drafting privacy notices

Providing privacy information is required under the Data Protection Legislation (the Legislation) and the General Data Protection Regulations (GDPR).

If collecting information for the first time that would entail large volumes of information or the information will be subject to large scale processing, you will need to consider preparing a Data Protection Impact Assessment (DPIA).

If the information collected falls within the Special Categories of Personal Information, the consent of the ICO will be required prior to the collection and processing.

Please see the guidance on Data Protection Impact Assessments for more information.

Individuals have the right to know **why** their personal information is required, **how** it is processed (used) and to have **control** over the purposes for which their information is processed and who it is shared with.

This should be established at the point at which personal information is obtained from individuals, explaining why the Council needs the information and requesting consent for processing, if consent is appropriate (more information on obtaining consent can be found in the Council's 'Guidance for Obtaining Consent'). Under the GDPR and the Legislation, the Council will find it more difficult to rely on consent and should not do so if it can rely on a lawful basis for processing. The Council should be clear on what the lawful basis for collecting and processing the information is, for example for the collection of taxes, and ensure that individuals are informed of this.

By communicating clearly with individuals, the Council can improve its reputation by showing that it values individuals' personal information, increasing public trust in the ways in which the Council handles their personal information.

When drafting a privacy notice you should ensure that you use clear, plain language aligned to the Council's 'house style.' You should be truthful and not provide individuals with misleading choices. For example, do not request consent for processing where, if consent is refused, you will process the information lawfully under a statutory power – this is misleading and unfair on the individuals concerned as they do not have a choice in whether or not the Council processes their personal information.

What to consider before drafting your Privacy Notice

1	**What personal information do you need?**	**Notes**
	What personal information are you requesting?	Be clear on the personal information you are requesting. Is the information adequate, relevant and not excessive?
	Why do you need it?	What is the **purpose** for which you are requesting this information? (*e.g. an individual wishes to report a missed bin collection and you required the individual's name and address in order to investigate their complaint)* Ensure that you only collect the minimum amount of personal information you require – do not obtain further personal information on a 'just in case' basis.
	What are you planning to do with this information?	How will you **process** this information? How long will the information be held for? Will the information be used for any other processing purposes? *(e.g. will the personal information be shared internally with other departments outside of the purposes of investigating the complaint?)*
2	**What rights does the individual have as to how their personal information is processed?**	
	The GDPR provides the following rights for individuals: 1. The right to be informed 2. The right of access 3. The right to rectification	Guidance on the rights of individuals as to how their personal information is processed is contained within Appendix 1. Many of the rights will be complied with under the Council's procedures for dealing with Subject Access Requests (SAR) and by ensuring that your privacy notice has provided all of the required information.

	4. The right to erasure 5. The right to restrict processing 6. The right to data portability 7. The right to object 8. Rights in relation to automated decision making and profiling	However, when requesting personal information from individuals you need to consider your legal basis for processing the information as it will have an effect on individuals' rights. For example, if you are relying on the consent of the individual for specific types of processing of their personal information, they will have stronger rights such as the right to have their information deleted (the right to erasure). Therefore before you request individuals' personal information it is crucial that you determine **and document** your legal basis for processing the information to ensure that you are informed about the rights individuals hold and your limits on the processing of their information *(e.g. consent can be withdrawn at any time, so you must be aware of this and have appropriate measures in place to document the withdrawn consent and to stop the processing of their personal information).* The Council has a duty under the GDPR/Leglislation to keep these records of processing activities which must be kept and updated to ensure that the Council is compliant with its duties.
3	**On what basis will you be processing the personal information?**	
	Do you have a statutory basis for processing the personal information? Will you use the information for a different purpose?	If you have a statutory basis empowering you to process the personal information, you will not need to rely on consent. **However,** will you process this information further than the purposes prescribed by the relevant statutory powers? In most circumstances, you will wish to process the personal information further – consider this when drafting any requests for personal information to determine whether a consent request is necessary – *it is advisable that you consider any further processing beforehand in order to request consent at the point that personal information is being obtained. If it is envisaged that further processing will take place, obtaining consent in the first instance will save the Council time, money and resources.*

	Do you need to rely on consent in order to process the personal information?	You are unlikely to require consent where the processing is necessary to carry out the transaction or deliver the service that the individual has requested. **However**, as explained above, where further processing is envisaged, it is desirable to obtain consent in the first instance prior to any further processing purposes that the Council identifies. If you are relying on consent, you must: • display your consent request clearly and distinctly – it must not be bundled up with other information such as terms and conditions. • ask individuals to display an affirmative action to opt-in – pre-ticked and opt-out boxes are prohibited and if used will not constitute valid consent. • provide specific information to allow the individual to make a clear and informed choice over how their personal information will be used. • explain the different purposes for which their information is required. • request separate and individual consent for each type of processing. • inform individuals of their right to withdraw consent and details of how to do so. You may also consider telling individuals what you will not do with their data and how you keep their data secure.
4	**Will you share the personal information?**	
	Do you need to share the information?	If so, is it clear to individuals that their information will be shared? Is it obvious that their information will be shared? *(E.g. that the individual's name and address will be shared with HTS to enable them to carry out Landlord repair works requested by the individual who is a secure tenant of the Council).*

		However, remember not to assume that everybody will have the same level of understanding or the same reasoning process as you – where it may be obvious to you, it may not to another. Therefore, where possible explain how the individual's personal information will be shared, even if it seems obvious.
	Do you share the personal information because Harlow Council has a statutory duty to do so?	In these circumstances you do not need to advise the data subject. However, it would be more open and transparent to do so. If the Council has a statutory duty to share information ensure that you are clear about which legislation requires disclosure and what information is required to be disclosed.
	Do you share the information with the Audit Commission for the data matching exercise (NFI)?	A fair processing notice will need to be included at the point at which the request for personal information is made.
	Do you share information for other reasons? Are you sharing the information with an external organisation? Are you sharing the information with an internal department?	You will need to check that the sharing of information is legal. Is there an information sharing agreement? What will the organisation (you are sharing the information with) do with the information and what effect will that have on the data subject? Where you are sharing within an internal department, you must ensure that you have a lawful basis for doing so, whether it is a statutory power or consent from the individual. Where you require personal information from another department or receive a request to share personal information, a personal data request form should be completed and sent to the Data Protection Officer to decide whether the sharing of the personal information would be fair and lawful processing or whether the consent of the individual is necessary.

5	**How long will you keep the personal information?**	
	Do you have a retention period for the personal information you collect? Are there statutory guidelines for how long the personal information should be retained? Do you follow any 'best practice' guidelines in regards to retaining personal information?	Retaining personal information for longer than necessary may be deemed to be excessive and irrelevant and therefore a breach of the Legislation/GDPR. Therefore it is important to consider how long you will retain the information for and inform individuals of this. Though there is no statutory basis for reviewing consent, it is best practice to review every two years and keep records of the reasons why you are still relying on the consent previously given or why the information is no longer required for that purpose. If the information is no longer required you should check the Council's Data Retention Policy to determine how long the information should be keep before being securely destroyed. **It is not acceptable to keep information indefinitely or "just in case" it is needed.**

Drafting your Privacy Notice

The GDPR requires Data Controllers to take 'appropriate measures' to inform individuals of how their information will be processed and places an emphasis on providing understandable and accessible privacy notices. The GDPR specifies that privacy notices must be:

- concise, transparent, intelligible and easily accessible;
- written in clear, plain language; and
- free of charge.

The GDPR includes a long and detailed list of the information that must be provided in a privacy notice and the Information Commissioner's Office (ICO) summarises the required information:

What information is required?	Data obtained directly from Individual	Data not obtained directly from Individual
Identity and contact details of the Data Controller and the Data Protection Officer	✓	✓
Purpose of the processing and the legal basis for the processing	✓	✓
The legitimate interests of the Data Controller or third party where applicable	✓	✓
Categories of personal information		✓
Any recipient or categories of recipients of the personal information	✓	✓
Details of transfers to third country and safeguards (if applicable)	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of the individual's rights in regards to how their information is processed	✓	✓
The right of the individual to withdraw consent at any time (where consent for processing is being relied upon)	✓	✓
The right to lodge a complaint with a supervisory authority (the ICO)	✓	✓
The source that the personal information originates from and whether it came from publicly accessible resources		✓
Whether the provisions of personal information is part of a statutory or contractual requirement/obligation and the possible consequences of failing to provide the personal information	✓	

The existence of any automated decision making, including profiling and how decisions are made, the significances and the consequences	✓	✓
When should the above information be provided to the individual concerned?	At the time that the information is obtained	Within a reasonable period since obtaining the information (one month) If the information is used to communicate with the individual, the information should be provided when the first communication takes place, at the latest If disclosure to another recipient is envisaged, the information should be provided before the information is disclosed at the latest

It is advisable to have a layered approach to privacy notices, to inform the individuals of the specific reasons why your department is collecting and processing information. These should be linked to the Council's main privacy notice.

Appendix 1

Data subject's rights under the GDPR

1. The Right to Transparency

The right to transparency is an integral part of the lawfulness, fairness and transparency principle. Individuals must be informed of the processing activities concerning their personal data, particularly where it involves profiling, in which case the individual will need to be informed of its potential consequences.

In order to comply with the right to transparency privacy notices must be clear and unambiguous, see above.

Transparency information need not be given in the following circumstances:

- The data subject is already aware of the processing activity.
- The recording or disclosing of personal information is expressly permitted by law, or
- Providing the information to the data subject would be impossible or involve disproportionate effort, (public interest in archiving, or scientific or historical research, taking into account the number of data subjects, the age of the data and the safeguards undertaken).

2. The Right to Information and Access to Personal Data

A data subject has a right to access information held about them by a data controller; for example contractors who are both data controllers and processors on behalf of the Council, a Councillor and any subsidiary of the Council.

The data controller must confirm to the data subject if they are processing their personal data and must also provide the following:

- The purpose of the processing.
- The categories of personal data held.
- The recipients of the personal data or categories of recipients.
- Whether any recipients or categories are located in third countries.
- Where possible the period for which the data will be stored, or where this is not possible the criteria for determining the retention period.

- The existence of the data subject's rights to rectification, erasure (in some circumstances), restrict processing and to object to processing.
- The right to complain to the supervisory authority [the Information Commissioner's Office].
- If data is not collected directly from the data subject, the source of the information.
- The existence of automated decision making and the logic involved in the decision making process.
- Details of any transfer to third countries, and the safeguards implemented regarding the transfer.

If possible data subjects should be given direct remote access to their personal data, this access should not compromise the data controller's or any third parties rights. Prior to disclosing any personal data the identity of the individual should be verified.

Data subject access requests should be responded to within twenty working days of receipt. This can be extended by two months if complex or numerous requests have been made, but the data controller must tell the data subject that they are going to apply the extension at the outset.

Normally no fee can be charged.

3. The Right to Rectification

The data subject has a right to ask for any inaccurate data to be rectified and that any incomplete data be completed taking into account the purpose of the processing, including by means of a supplemental statement.

If the data has been shared with third parties, the data controller must inform them of the rectification unless doing so would involve a disproportionate effort or be impossible.

4. The Right to Erasure (the right to be forgotten)

The right to erasure is not an absolute right. Data subjects have a right to be forgotten if their personal data is no longer required for the purposes for which it was collected. This is particularly relevant to on-line collection especially if the data relates to a child. The right to erasure does not apply if there is a lawful reason for continued processing.

The GDPR imposes an obligation on data controllers to erase personal data concerning a data subject without delay in the following circumstances:

- The personal data is no longer required for the purpose for which it was collected.

- The data subject withdraws consent and there is no other lawful basis for processing.
- The data subject objects to processing (see below).
- The personal data has been unlawfully processed.
- The personal data must be erased pursuant to a legal obligation to which the data controller is subject.
- The personal data has been collected in relation to an offer of “information society services” to a child.

If the personal data has been shared with other data controllers they must be informed of the request and informed that they must erase any links or copies of the data subject’s personal data. Reasonable steps need to be taken to erase personal data made public, taking into account cost and technology and you must also inform other data controllers who have access to the information made pubic of the request for erasure.

Exemptions to the right of erasure:

- Exercising the right to freedom of expression and information.
- Compliance with a legal obligation which the data controller is subject to, or for the performance of a task in the public interest.
- Any reason of public interest in public health.
- Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- For the establishment, exercise or defence of legal claims.

Records of requests need to be documented to comply with the accountability principle within the records of processing activity.

5. The Right to Restrict Processing

This is a new right introduced by the GDPR, giving data subjects the right to restrict processing in the following circumstances:

- Where the data subject contests the accuracy of their personal data, processing can be restricted for a period to enable the data controller to verify whether the data is accurate.
- Where the processing is unlawful and the data subject opposes erasure and requests restrictions on processing instead.
- The data controller no longer needs the personal data for the purpose of its processing, but the data subject requires the personal data for the establishing, exercising or defending legal claims.

- Where the data subject has exercised the right to object to processing, see below, processing may be restricted for the period necessary to ascertain whether the data controller's legitimate grounds for processing override those of the data subject.

Where the data subject exercises this right, apart from storage, the affected personal data can only be processed:

- With the data subject's consent.
- For establishing, exercising or defending legal claims.
- For the protection of another natural or legal person's rights, or
- For reasons of important public interest of the Union or a Member State.

The data controller must tell the data subject before lifting the restriction of processing; they must also inform any third parties that they have shared the data with the identity of the personal data subject to the restriction.

In order to ensure that the right to restrict processing is complied with the data controller should restrict access to the identified personal data, move the data to another system, not process if it is in an automated filing system and mark it as being restricted and remove the data from the website.

6. The Right to Data Portability

This is a new right introduced by the GDPR, giving data subjects the right to receive their personal data from the data controller and to re-use it with another service provider. The right only applies to data processing by automated means that is necessary for the performance of a contract, or data processing on the basis of the data subject's consent. The right enables a data subject to instruct a data controller to transfer their data to another data controller if feasible.

The right to data portability is without prejudice to other data subject rights including the right to erasure. The right does not apply if the personal data is processed for the performance of a task in the public interest or in the data controller's official authority and must not affect the rights of others.

The main aim of the right to data portability is to facilitate the switching from one service provider to another e.g. gas suppliers. The data subject is entitled to receive the personal data they provided to the data controller in a structured, commonly used, machine readable format and to transmit the data to another data controller easily.

It does not mean that a data controller should keep personal data for longer than is needed just in case a request is made.

The data controller must provide the requested personal data within one month, unless the request is complex where a maximum of three months is allowed, from the date of the request.

7. The Right to Object to Processing

The right to object to processing operates differently in each circumstance, particularly with regard to the data controller's ability to refuse.

The data controller must respond to a request within one month of receipt, this can be extended by two months if the request is complex or numerous requests are received.

The right to object arises in the following circumstances:

- Processing based on the data controller's legitimate interests (not available to the Council as a ground for processing), the performance of a task carried out in the public interest or the exercise of official authority.
- Processing for the purpose of direct marketing.
- Processing for scientific, historical research purposes or statistical purposes.

On receipt of a request the data controller must stop processing unless it is able to demonstrate that processing is necessary for establishing, exercising or defending legal claims.

If the processing is for direct marketing purposes, including profiling, the data controller must cease processing and there are no grounds for a data controller to refuse to comply with such a request.

Where personal data is processed for scientific or historical research or statistical purposes, the data controller should cease processing unless it is in the public interest to continue to process.

The data subject must be informed of their right to object at the time of collection of personal data. If an on-line form is used then an on-line means of objecting must be provided.

8. Rights in relation to Automatic Decision Taking

This right refers to decisions made entirely by technological means without human intervention. Individuals have the right not to be subject to a decision based solely on an automated process where the result of processing has a legal, or similar, significant effect. Automated decision making includes profiling, i.e. any automated processing for the purpose of evaluating individuals.

An exemption to this right occurs where:

- The processing is necessary for the entering into, or the performance of, a contract between the subject and the data controller (e.g. an employment contract).
- The data controller is authorised to undertake the processing and has in place appropriate safeguards, e.g. fraud.
- The data subject has given explicit consent to the processing (see Council's guidance on consent for an explanation of explicit consent).

The data controller should give the data subject the right of human intervention in the decision making process, to be able to express their views and the means to contest the automated decision.

The above exemptions do not apply if the data subject is a child, or to the special categories of personal data, unless the data subject has given explicit consent to the automated decision making process, or the processing is for reasons of substantial public interest.