By answering this question you will understand:

* if you are allowed to collect information.
* the process for collecting information on behalf of London Borough of Hackney.

**We are all responsible**

It is your responsibility to ensure that you:

* question whether personal information is needed, and how much personal information is needed in the scope of your work.
* provide an appropriate privacy notice when collecting information.
* record information accurately.
* only collect the information that is relevant to your work.

**Informing people about why their information is being collected, and how it will be used**

The asset (for example, council employee records) or application (the HR system) you manage may process personal information that has been collected online, on the phone or in person. In the course of collecting this information, it is important that you ensure a privacy notice has been issued.

Privacy notices can be read out to the member of the public, or published in print or online. Whatever method is relevant to your project or service.

Privacy notices must be:

* concise, transparent and easy to hear or read.
* written in clear and plain language, particularly if addressed to a child.
* free (you can’t charge a fee to the person from whom you are collecting the information, for them to access the privacy notice).
* kept up to date if or when the use of that information changes.

You do not need to obtain evidence (for example through a tick box) that the user has read or understood the privacy information.

**Example of a privacy notice**

This is an example of a privacy notice:

The Council will use personal data about you for the enforcement of parking and traffic contraventions and other compatible purposes.

This may be collected from you, or from other organisations. If the data is obtained from other organisations, this is done in accordance with data protection legislation.

You can read more information about this, and also about your Data Protection rights in line with the provisions of the General Data Protection Regulations and Data Protection Act 2018 by going to<https://www.hackney.gov.uk/privacy>. This includes how to contact the Data Protection Officer, how long your information is held, and how we process your personal information. Printed copies of the Council’s Privacy Notices can be provided on request.

The Council will:

* use personal data about you for the purpose of performing any of its statutory duties or public tasks.
* make any disclosures required by law and may also share this information, both across council departments and with other local authorities and government organisations.
* check information you have provided, or information about you that someone else has provided, with other information it holds.

The Council will not give information about you to anyone else, or use information about you for other purposes, unless the law allows this.

**Record information accurately and professionally, and only collect as much as you need**

You must make sure information is recorded accurately and professionally, even if it is for internal use. This information could be published in the public domain at a later date.

The Council is a data controller and responsible for ensuring that all personal information is collected and processed lawfully and securely. The Council wants to avoid excessive and unnecessary information collection to protect and respect our residents’ privacy.

It is important to keep this principle in mind when collecting information for the project or service you are working on.

#### **Personal observations**

There are no set rules about what data is is right or wrong to collect, as it will depend on the context of the service you are delivering. For example in some cases it might be excessive to note down personal opinion or observation, but for some services this might be an essential part of their job.

You should always work in line with standards for your service, and consider whether you need the data that you are recording.

**An example of when not to collect personal information**

A member of the facilities management team is at a block of flats to follow up on a complaint about a faulty lift.

A resident in the block notices the Council employee and stops to talk to them, confirming the issue about the lift, when it occurs and adds how long the problem has been going on.

It would be appropriate to take note of this helpful information about the lift from the resident, and you should do so anonymously if their name and address is not required.

You may decide to ask them if they are happy for you to record their name and address if this will assist in resolving the issue. You need to carefully consider whether it is appropriate to record the fact that they are disabled as this information is sensitive and should not be collected without a clear purpose.

You should be careful not to collect personal data ‘invisibly’ (without the person knowing that you are through provision of privacy information) unless this is necessary as part of the service that you are providing.

**If you need to collect more information**

You may think you have a justified reason for collecting additional extra information from people who use your service, or from staff. Examples of this are collecting location data of staff using Council vehicles or devices, or adding a mandatory field requesting disability status when someone makes a Freedom of Information request.

The Council has a three step process to follow when considering gathering new information.

It’s important you understand this process because there are serious implications for you and the Council if we start collecting new data without considering the implications and methods carefully first.

#### **Step 1: Check - are you collecting new information?**

Perhaps this information is already available from a colleague. If so, can you justify why you should have access?

If the information you need to collect isn’t available elsewhere, how much information do you really need to ask people to provide?

#### **Step 2: Ensure that a Privacy Impact Assessment is carried out.**

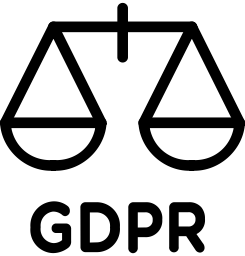
There is a short set of screening questions that will indicate whether you need to do a full Privacy Impact Assessment. If you do, it is not a form filling exercise but is a consultation process that identifies and reduces privacy risks. It includes the following steps:

1. identify the need for a Privacy Impact Assessment
2. describe what you want to do with the information
3. identify the privacy and related risks
4. identify and evaluate the privacy solutions
5. consult with internal and external stakeholders as needed throughout the process (it is mandatory to consult the Data Protection Officer and if there are high risks you may need to consult the Information Commissioner’s Office).

As someone with responsibilities for making decisions about the way information is managed, you may be a key stakeholder in the PIA process. At the Council there are some advisory roles (such as the Data Protection Officer, and Legal) but the Information Asset Owner makes the final decision.

#### **Step 3: The outcomes of the PIA must be recorded and signed off, and integrated into the project plan.**

**Processing personal information lawfully**



We are all required to process personal information lawfully, fairly and in a transparent manner. Processing is only lawful if you can prove a ‘lawful basis’ and identifying this is a key consideration during the Privacy Impact Assessment before collecting new data.

There are six available lawful bases for processing:

1. Consent: the individual has given clear consent for you to process their personal information for a specific purpose.
2. 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.
3. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
4. Vital interests: the processing is necessary to protect someone’s life.
5. 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.
6. 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 information which overrides those legitimate interests (This cannot apply to the Council, as a public authority processing information to perform official tasks).

Where possible we should not rely on 'consent' as it is more difficult for us to demonstrate that consent is freely given for any of our core services. 'Legitimate interest' is also less relevant to us as a public body. In most cases we would expect the lawful basis of processing to be either ‘legal obligation’ or ‘public task’ as part of the Council carrying out its duties.

You must, however, be able to demonstrate that the processing of personal information is justified and it may be necessary to use different lawful bases for processing for different sets of information you manage. For example, a local college might rely on ‘public task’ for processing personal information for teaching and research purposes; but a mixture of ‘legitimate interests’ and ‘consent’ for alumni relations and fundraising purposes.

The lawful basis for processing must be recorded in the Council’s Information Asset Register and this can’t be changed retrospectively. For example, if the Council’s Asset Register says the information is processed based on consent and a member of the public decides to withdraw their consent, the Council can’t then decide to change the lawful basis to ‘legal obligation’ to avoid having to stop processing their data.

**Obtaining consent for processing personal information**

There will still be some cases when you have to ask for consent. In addition to collecting personal data, this might be the case when you want to give people the chance to opt-in to newsletters.

To meet the standard of consent, you must provide:

1. a positive opt-in, not pre-ticked boxes or methods of default consent.
2. a very clear and specific statement of consent.
3. separation from other terms and conditions.
4. requests for consent for separate things. Vague or blanket consent is not acceptable.
5. clarity, be clear about what you are asking for and keep it concise.
6. name any third party controllers who will rely on the consent.
7. make it easy for people to withdraw consent and tell them how.
8. keep evidence of consent – who, when, how, and what you told people.

For example, if a member of the public contacts Sport, Leisure & Physical Activity Development to enquire about a facility for hire, the Council cannot then retain their contact details to market sports and leisure activities to them at a later date. The member of public would have to actively sign up to receive marketing information about the facilities and sports, before they could be contacted about these things.

**Does your role require you to collect information about children?**

If you collect personal information about children, it is important that you understand how GDPR could impact the collection and processing of this information. Children are less likely to be aware of the risks involved in the collection and sharing of information, so GDPR requires us all to design our processes and systems with their protection in mind.

You will need to have a lawful basis for processing a child’s personal information.

When considering the lawful basis for processing of children’s data, the same considerations apply as with any data that we are processing - for example that for our core services ‘legal obligation’ and ‘public task’ will most likely apply.

However, there may be cases where consent is the best option available. There are a few other things to consider with data about children:

* only children aged 13 years or over are able to provide their own consent for an online service.
* for children under 13 years, you must get consent from whoever holds parental responsibility for the child - unless the online service you offer is a preventive or counselling service.
* specific care and protection is required if you are using children's personal information for marketing purposes, or creating user profiles.
* do not make decisions based solely on automated processing about children if this will have a legal or similarly significant effect on them.
* write clear privacy notices for children so that they are able to understand what will happen to their personal information, and what rights they have.
* children have the same rights as adults over their personal information. These include the rights to access their personal information; request rectification; object to processing and have their personal information erased.
* an individual’s right to erasure is particularly relevant if they gave their consent to processing when they were a child.

**Tasks**

Basic

**Gathering personal information**

Think of a service or project where you are required to gather personal information. Describe three things you will check before gathering information

Indermediate

**Lawful bases for processing**

Name two lawful bases for processing that are relevant to your department.

Advanced

**Collecting information about children**

How old must a child be to provide their own consent for an online service and are there any exceptions?