GDPR Overview

1. What is Personal Information?

There are two categories of personal information – Personal Information and Special Categories of Personal Information (previously referred to as sensitive personal information).

Personal Information

"Personal information" is any information that identifies, or is capable of identifying, any **living** person. This includes any references to names, identification numbers linked to individuals, location data and online identifiers such as IP addresses. It also includes information regarding an individual's physical or mental state as well as social or cultural information relating to an individual.

Special Categories of Personal Information

"Special category personal information" is information that can be considered to be more sensitive information about individuals, and therefore requires more protection. This includes information that identifies an individual's racial/ethnic origin, political opinions, religious/philosophical beliefs, sexual orientation and information regarding an individual's health.

We must only use the personal information where we have a **lawful basis for processing** (discussed below) and for the purpose(s) for which we told the individuals we would use it when we collected it from them. We must also keep the information secure, keep it for no longer than is necessary and ensure that we do not collect excessive amounts of personal information – more information on how the Council must treat personal information can be found in the Council's main Privacy Notice and the Right to be Informed (discussed below).

When we are collecting information falling within the special categories of personal information, we must obtain the **explicit consent** of the individuals, except in very limited circumstances – Guidance on Obtaining Consents has been produced and published on the Infonet, and if you intend to collect this kind of information, please seek the advice of the Council's Data Protection Officer (DPO) – data.protection@harlow.gov.uk

2. Lawful basis for processing

In order to legally process personal information under the GDPR, we MUST have a lawful basis for processing.

There are a number of lawful bases for processing, however the most relevant to Harlow Council are:-

For personal information

To comply with a legal obligation that the Council is subject to (Article 6(1)(c) GDPR).

For the performance of a task carried out in the public interest or in the exercise of official duty vested in Harlow Council (Article 6(1)(e) GDPR).

For the performance of a contract or to take necessary steps to enter into a contract with the individual (Article 6(1)(b) GDPR) – this includes providing a service requested by the individual.

Where we have the individual's consent to do so (Article 6(1)(a) GDPR) - for more information on obtaining consent - including the requirement that it must be as easy for an individual to **withdraw their consent** as it is to provide it -please see the Guidance for Obtaining Consent on the Infonet.

Where it is necessary for the purposes of the legitimate interests pursued by Harlow Council except where such interests are overridden by the interests, rights and freedoms of the individual (Article 6(1)(f) GDPR) – this may only be used by Local Authorities in limited circumstances and advice should be sought from the Council's Data Protection Officer (DPO) if you consider this to be your lawful basis for processing – data.protection@harlow.gov.uk

Where it is necessary in order to protect the vital interests (meaning a life or limb situation) of the individual or another individual (Article 6(1)(d) GDPR) – this is likely to only occur in rare circumstances and advice should be sought from the Council's Data Protection Officer (DPO) if you consider this to be your lawful basis for processing data.protection@harlow.gov.uk

For special categories of personal information

Where we have the individual's explicit consent to do so (Article 9(2)(a) GDPR) - for more information on obtaining consent please see the Guidance for Obtaining Consent on the Infonet.

Where the processing relates to personal information that has been manifestly made public by the individual (Article 9(2)(e) GDPR)

Where it is necessary for the establishment, exercise or defence of legal claims or when we are compelled by the Courts to do so (Article 9(2)(f) GDPR).

Where is it necessary for the purposes of carrying out obligations of Harlow Council in the field of employment or social security **(for Harlow Council Employees)** (Article 9(2)(b) GDPR).

Where it is necessary for the purposes of preventive or occupational medicine pursuant to a contract with a health professional **(for Harlow Council Employees)** (Article 9(2)(h) GDPR).

Where it is necessary in order to protect the vital interests (meaning a life or limb situation) of the individual or another individual (Article 9(2)(d) GDPR) – this is likely to only occur in rare circumstances and advice should be sought from the Council's Data Protection Officer (DPO) if you consider this to be your lawful basis for processing data.protection@harlow.gov.uk

3. Data Protection: Individuals' Rights and when they apply

Individual Rights	Does it always apply?
1. The right to be informed	✓
2. The right of access	✓
3. The right to rectification	✓
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	✓

For more information on what these rights mean, the circumstances in which they apply and complying with them, please see below.

Individuals' Right	What does this mean?	When does this apply?
1. The right to be informed	• This is a key transparency requirement under the GDPR and the best way of complying is with the use of privacy notices (discussed below). • This is about informing people about why we are collecting their personal information and what we are using it for. • This information should be provided to individuals at the point we collect their information (such as on a form we are asking them to complete). • If we receive personal information about someone from a third party, we need to inform the individual within a reasonable time of receiving it and in any event no later than one month. • The information we provide must be in concise, intelligible and in clear and plain language so that it can easily be understood by individuals.	ALWAYS Individuals must always be informed of why we are collecting their information and what we are using it for (including who it will or may be shared with both internally and externally). For more information on privacy notices please see the section below, as well as the Guidance for drafting Privacy Notices on the Infonet and the Council's main Privacy Notice. A Data Sharing Request Form and a Data Sharing Decision Form has been created and published on the Infonet to be used by for internal data sharing of personal information from department to department.
2. The right of access	Personal information is just that: information relating to an individual, and therefore people should be allowed to see it. The right of access does this by entitling individuals to the following information: • Confirmation that their personal information is being processed	ALWAYS This right exists for all individuals and upon an individual making a SAR, we must comply within one month of receiving the request. SARs can only be refused in **very limited** circumstances.

	• Access to their personal information that we hold • Information largely contained within the privacy notice such as the lawful basis for processing, who it will be shared with and how long we will keep it for and so on. This information must be provided free of charge, but reasonable fees based on the administrative cost of providing the information may be applied in limited circumstances. The method by which this right can be exercised is by way of a Subject Access Request (SAR) (more information can be found in Section 7 of the Access to Information Policy).	
3. The right to rectification	This gives individuals to have their personal information held by the Council rectified or, if it is incomplete, the right to have it completed. Personal information is inaccurate if it is incorrect or misleading as to any matter of fact. Even where you took steps to ensure the accuracy of the information when it was collected, you must reconsider its accuracy on request by the individual. Where opinion about the individual is the information that is being disputed, the record must clearly show that the information is opinion and whose opinion it is (where appropriate). As opinions are subjective, it may be difficult to say that it	<u>ALWAYS</u> The right exists for all individuals and can be requested verbally or in writing and the Council must respond within one month. Where requests are received verbally, we must take a record of the request and confirm with the requestor that the record is accurate. Once in receipt of the request, the Council must restrict its processing of that personal information whilst it is investigating whether the information is inaccurate or not – please see the right to restrict processing below.

	is inaccurate and needs to be rectified.	If satisfied that the information **is accurate**, we should inform the individual of this and that we will not be amending the information. We should explain the reasons for our decision and inform them of their right to complain to the ICO, as well as their ability to enforce their rights through the Courts. Where we agree that the information **is inaccurate**, we should inform the individual of this and explain how the information will be rectified, e.g. what the personal information now states. When receiving and responding to a request, a note should be placed on our systems recording that the individual made the request, their reasons, and our final decision. A request can only be refused in **very limited** circumstances.
4. The right to erasure	This is also known as 'the right to be forgotten' and gives individuals the right to have their personal information erased, in the following **limited circumstances**: • the personal information is no longer necessary for the purpose for which we originally collected or processed it for; • we are relying on the individual's consent as our lawful basis for holding the information, and the individual withdraws their consent;	NOT ALWAYS The right exists for all individuals in the limited circumstances (listed to the left) and can be requested verbally or in writing and the Council must respond within one month – this can be extended by a further two months where the request is complex so long as the individual is informed of the extension and why it is necessary. Where requests are received verbally, we must take a record of the request and confirm with the requestor that the record

	• we are relying on legitimate interests as our basis for processing, and the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing; • we are processing the personal data for direct marketing purposes and the individual objects to that processing; • we have processed the personal data unlawfully under the Data Protection legislation; or • we have to do it to comply with a legal obligation; or • we have processed the personal data to offer information society services to a child.	is accurate. Once in receipt of the request, the Council must restrict its processing of that personal information whilst it is investigate whether the information can and should be deleted – please see the right to restrict processing below. If satisfied that the information **cannot be deleted**, we should inform the individual of this. We should explain the reasons for our decision and inform them of their right to complain to the ICO, as well as their ability to enforce their rights through the Courts. Where we agree that the information **can and should be deleted**, we should inform the individual of this and explain how and when the information will be deleted, e.g. deletion by shredding and the date of deletion OR a reasonable timescale for deletion. Where we have erased personal information that: **1. we have disclosed to others** • we must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, we must also inform the individuals about these recipients; and/or

		2. that personal information has been made public in an online environment • we must take reasonable steps to inform other controllers who are processing the personal data to erase links to, copies or replication of that information, taking into account available technology and the cost of implementation. When receiving and responding to a request, a note should be placed on our systems recording that the individual made the request, their reasons, and our final decision. A request can only be refused in **very limited** circumstances, such as the processing of the personal information being necessary in order for the Council to fulfil a legal obligation.
5. The right to restrict processing	Individuals have the right to restrict the processing of their personal data by the Council in the following **limited circumstances**: • the individual is challenging the accuracy of their personal information and you are verifying the accuracy of it as per their request (discussed above); • the personal information has been unlawfully processed and the individual opposes erasure and requests restriction instead;	NOT ALWAYS The right exists for all individuals in the limited circumstances (listed to the left) and can be requested verbally or in writing and the Council must respond within one month – this can be extended by a further two months where the request is complex so long as the individual is informed of the extension and why it is necessary. Where requests are received verbally, we must take a record of the request and confirm with the requestor that the record is accurate.

	• you no longer need the personal information but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or • the individual has objected to you processing their information (as referred to below), and you are considering whether your legitimate grounds override those of the individual.	Once in receipt of the request, we must be able to restrict processing, by (for example) temporarily moving the personal information to another processing system; making it unavailable to users; or temporarily removing published personal information from our website – this is another reason why it is important to know what personal information we hold and where it is stored to enable us to act quickly to comply with our legal obligations on receipt of a request. Once the personal information is restricted we cannot use it in any way (other than the store it) unless: • we have the individual's consent to do so; • the personal information must be processed for the establishment, exercise or defence of legal claims; • it must be processed to protect the rights of another individual; or • it is for reasons of important public interest. Where we have disclosed personal information being restricted to others, we must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, we must also inform the individuals about these recipients The restriction can be lifted where (a) it was placed on the personal information

		whilst we investigated the accuracy of the personal information at the request of the individual or (b) where the individual has objected to our processing of their personal information on the basis that it is necessary for the performance of a public task or to carry out our legitimate interests and have decides that these override those of the individual. **However,** where we decide to lift a restriction we **must** inform the individual **before** we do so, informing them of the reasons for our decision, of their right to complain to the ICO, as well as their ability to enforce their rights through the Courts. When receiving and responding to a request, a note should be placed on our systems recording that the individual made the request, their reasons, and our final decision. A request can only be refused in **very limited** circumstances.
6. The right to data portability	This allows individuals to obtain and re-use their personal information for their own purposes across different services by moving, copying or transferring it easily from one IT environment to another in a safe and secure way, without hindering its usability. For example, where an individual moves to a new banking provider and asks that their banking history is sent to them by their old provides.	NOT ALWAYS The right exists for all individuals in the limited circumstances (listed to the left) and the Council must respond within one month – this can be extended by a further two months where the request is complex so long as the individual is informed of the extension and why it is necessary.

	The right only applies: • to personal information an individual has provided to us; • where the processing is based on the individual's consent or for the performance of a contract; and • where processing is carried out by automated means (referred to below).	To comply with our legal obligations we must provide the personal information in a structured, commonly used and machine-readable form (including CSV files). It must be provided free of charge and, if the individual requests it, we may be required to transmit the data directly to another organisation if this is technically feasible, without adopting/maintaining processing systems that are technically compatible with other organisations. Where we will not take action in response to a request, we <u>MUST</u> inform the individual of the reasons for our decision, of their right to complain to the ICO, as well as their ability to enforce their rights through the Courts. When receiving and responding to a request, a note should be placed on our systems recording that the individual made the request, their reasons, and our final decision.
7. The right to object	Individuals have the right to object to: • the processing of their personal information based on legitimate interests or the performance of a task in the public interest/the exercise of official authority (including profiling discussed below) where they have on "grounds relating to her or her situation";	<u>NOT ALWAYS</u> The right exists for all individuals in the limited circumstances (listed to the left). To comply with our legal obligations **<u>where we process personal information for the performance of a legal task/for our legitimate interests</u>** we must stop processing the personal information <u>UNLESS:</u>

	• direct marketing (including profiling); and • the processing of their personal information for the purposes of scientific/historical research and statistics.	• we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individuals; or • the processing of the personal information is necessary for the establishment, exercise or defence of legal claims. To comply with our legal obligations **where we process personal information for direct marketing purposes**, we must STOP processing as soon as we receive an objection – there are no circumstances when a request of this type can be refused. To comply with our legal obligations **where we process personal information for research purposes**, the individual MUST have "grounds relating to his or her situation" in order for us to stop the processing. If we are conducting research where the processing of personal data is necessary for the performance of a public interest task, we are NOT required to comply with the individual's objection. If we carry out any of the above processing activities online, we MUST offer a way for individuals to object online. The right to object must be contained within our privacy notice to the individual (referred to above within the Right to be

		Informed).
8. Rights in relation to automated decision-making and profiling	**Automated individual decision-making** is the processing of personal information whereby a decision is made solely by automated means WITHOUT any human interaction. This is restricted where it has legal or similarly significant effects on the individual. **Profiling** is the processing of personal information by automated means for the purpose of evaluating certain things about the individual. We can only carry out these types of processing where the decision is: • Necessary for the entry into or the performance of a contract; or • Authorised by any applicable EU law; or • Based on the individual's EXPLICIT consent.	ALWAYS We can only use these types of processing for the reasons listed to the left and a **Data Protection Impact Assessment (DPIA)** MUST be carried out to consider and address any risks to individuals prior to introducing any new automated decision-making or profiling. To comply with our legal obligations, we must provide individuals with specific information about: • The processing of their personal information (e.g. the logic as to how the decision is made); AND • How they can request human interaction or challenge a decision. Additionally, we MUST carry out regular checks to make sure that our systems are working intended (e.g. take steps to prevent errors, bias and discrimination). This information should be contained within our privacy notice to the individual (referred to above within the Right to be Informed), along with the individuals' Right to Object (above).

3. Contracts and GDPR

If the Council is entering into a contract which will involve the sharing of personal information and/or special categories of personal information, a written contract MUST be in place which contains specific provisions in relation to:

- The subject matter and duration of the processing;
- The nature and purpose of the processing;
- The type of personal information and the categories of data subjects; and
- The obligations and rights of the data controller.

The contract MUST state that the processor must:

- only act on the written instructions of the controller (unless required by law to act without such instructions);
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage a sub-processor with the prior consent of the data controller and a written contract;
- assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- securely delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their GDPR obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

As a matter of good practice, the contract should:

- state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR; and
- reflect any indemnity that has been agreed.

For more information please see the briefing paper regarding Data Processors Contractual Obligations.

It may also be necessary to enter into a Data Sharing Agreement/Protocol and a template is available on the Infonet HERE. Once complete this should be sent to the Council's DPO via email to data.protection@harlow.gov.uk

Where the performance of the contract will involve the processing of large volumes of personal information or is for the implementation of a new system, a Data Protection Impact Assessment (DPIA) is required (discussed below).

4. Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment is a process to help us identify and minimise the data protection risks of a project. DPIAs MUST be carried out for certain types of processing AND for any other processing that is likely to result in a high risk to individuals' interests.

A DPIA MUST:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals by considering both the likelihood and the severity of any impact on individuals; and
- identify any additional measures to mitigate those risks.

We MUST carry out a DPIA where we are planning to:

- use profiling or automated decision-making to make significant decisions about individuals;
- systematically monitor a publicly accessible place on a large scale;
- use new technologies;
- use profiling, automated decision-making or special category personal information to help make decisions on someone's access to a service, opportunity or benefit;
- carry out large scale profiling;
- combine, compare or match data from multiple sources;
- process personal information without providing a privacy notice directly to the individual;
- process personal information in a way which involves tracking individuals' online or offline location or behaviour.
- process children's personal information for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- process personal information which could result in a risk of physical harm in the event of a security breach.

There are other circumstances in which we MUST or SHOULD CONSIDER carrying out a DPIA and guidance should be sought from the Council's DPO at data.protection@harlow.gov.uk .

5. Glossary

'Consent' means any freely given, specific, informed and unambiguous indication of the Data Subject's agreement, made by a statement of clear affirmative action, to the processing of their personal information by the Council.

'Data Controller' means the person or authority/body that determines the purposes and means of processing personal information.

'Data Processor' means the person or authority/body that is responsible for processing personal information on behalf of a Data Controller.

'Data Protection Impact Assessment (DPIA)' means the documenting of the process by which you identify any data protection risks of a project and how to minimise or eliminate those risks.

'DPO' means the Data Protection Officer, which the Council MUST have. The DPO is here to assist the Council to monitor internal compliance, inform and advise on our data protection obligations and to help demonstrate compliance with them, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for Data Subjects and the supervisory authority (ICO). The DPO MUST be independent, an expert in data protection, adequately resourced, and report to the highest management level.

'Data Subject' means an individual who is the SUBJECT of the information – the information is ABOUT them and is PERSONAL to them.

'GDPR' means the General Data Protection Regulation 2016/679

'ICO' means the Information Commissioner's Office which is the relevant supervisory authority in the UK.

'Personal Information' means any information relating to an identifiable **living** person who can be directly or indirectly identified in particular by reference to an identifier (e.g. name, identification number, location data or online identifier).

'Processing' means any operation(s) which is performed on personal information such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, disclosing, restricting, erasing, destroying or otherwise using the personal information.

'Special Categories of Personal Information' means sensitive personal information relating to an identifiable **living** person who can be directly or indirectly identified in particular by reference to an identifier (e.g. race, ethnic origin, political opinions/allegiances, religious beliefs, trade union membership, genetic, biometric data, physical and mental health, sex life and sexual orientation).

6. Additional sources for guidance

Useful guidance is available on the ICO website at https://ico.org.uk/for-organisations/

The Council's main Privacy Notice - http://www.harlow.gov.uk/privacy-notice

The GDPR Infonet page - http://infonet.harlow.gov.uk/infonet/gdpr

Guidance for drafting Privacy Notices - http://infonet.harlow.gov.uk/system/files/Guidance%20for%20Drafting%20Privacy%20Notices.pdf

Guidance for Obtaining Consents - http://infonet.harlow.gov.uk/system/files/Guidance%20for%20Obtaining%20Consents.pdf

Data Sharing Agreement/Protocol template - http://infonet.harlow.gov.uk/system/files/Information%20Sharing%20Protocol.pdf

Internal Data Sharing Request form - http://infonet.harlow.gov.uk/system/files/Harlow%20Internal%20Data%20Sharing%20Request%20Form.pdf

Internal Data Sharing Decision form - http://infonet.harlow.gov.uk/system/files/Harlow%20Internal%20Data%20Sharing%20Decision%20Form.pdf

Harlow Council's Data Breach Policy - http://infonet.harlow.gov.uk/system/files/Data%20Breach%20Policy.pdf