Article 30 Declaration Enfield Council

What is this document?

The General Data Protection Regulation 2016 (GDPR) as enacted in the UK by the Data Protection Act 2018 requires that all data controllers and processors publish a record of processing (GDPR Article 30 Clause 1). This document provides this for our council.

(a) The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

The data controller is Enfield Council with contact details:

complaintsandinformation@enfield.gov.uk

or by post:

Complaints and Information
Enfield Council
Civic Offices
Silver Street
Enfield
EN1 3XA

The Data Protection Officer may be contacted by email:

Enfield.Data.Protection.Officer@enfield.gov.uk

or by post:

Data Protection Officer
Enfield Council
Civic Offices
Silver Street
Enfield
EN1 3XA

(b) the purposes of the processing;

Data is used in Enfield Council in accordance with our published privacy statement. Specifically, we process data in order to:

- Provide you with services, either as required by law (e.g. collection of council tax, provision of housing benefit) or as requested by you
- Communicate with you as required by law and, with your consent, tell you about services and events you have asked us to
- Carry out our legal responsibilities
- Plan our services
- Personalise our services to you

(c) a description of the categories of data subjects and of the categories of personal data;

We keep data about the following classes of people:

- Residents in the council area including any persons accessing council services
- People who register on our website

- Our workforce and people we interact with as part of our delivery

The types of data we collect are detailed in our published privacy statement. There are some specific areas in the privacy statement where we collect additional data not noted below. Generally, we collect:

Name and contact details: we collect your name, your address, your email address, your phone number and similar contact details. These are used to provide you with services and to contact you in relation to services. If you have given permission, we also use these for marketing purposes for services/events provided by us or by others in the local area. If you have given permission for third party marketing, we additionally may pass this data to third parties for carefully selected marketing relevant to

Demographic data: this includes age and gender. We may collect more sensitive characteristics such as nationality, race, religion, sexuality and ethnicity in order to fulfil our obligations under the Equalities Act 2010. These sensitive characteristics are only used for the purposes of the Equalities Act or those defined and to which you consented at the time we collected them. Where practicable, these data are managed separately from other data.

We additionally receive demographic data including aggregated data from other services to inform our planning of services. This data is not personally identifiable – we cannot identify individuals from the data, but will include matters such as health, police information and financial information.

Device and Usage data: when you connect to us online, we collect data about pages you have visited, completed actions, error messages, IP address details, device operating system, region and language settings. These are used to provide services to you, and to improve our services.

Preferences and account data: our systems include the ability to create an account using a username/password. The username is stored to allow us to retrieve your account; the password is NOT stored, but a “hashed” version of it is stored. This “hashed” password cannot converted back into your password, but allows our systems to confirm the correct password has been entered.

If you have created an account, we will store data in all the categories referenced elsewhere in this document with your account. This allows us to retrieve this data to auto-fill forms for you and present you with data about your past requests to us.

As an alternative, you may use a guest logon. This allows you to create a request to us, but the data given is only held in respect of that request. You cannot add more requests or retrieve history under a guest logon. Guest logons are valid only for the creation of a request and cannot be reused.

Financial Data: we collect data about income, outgoings, savings and assets owned in order to provide services to you. These include matters such as benefits and provision of social care.

We additionally receive financial data about you from third parties eg credit rating agencies.

Health and Care Data: we collect data about your health, including medical conditions, disabilities and information from your healthcare providers where needed to provide services to you.

We additionally receive health data about you from third parties eg NHS and police under a series of multi-agency sharing agreements. Data about you is used to inform our services to you and is only shared with practitioners in those services.

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

We disclose data to the following categories of recipients:

- The data subjects
- Parents / carers of data subjects where required by law
- Central government
- Health and Social Care
- Police
- We share your data with your consent or as necessary to provide any service.
- We share with third party organisations delivering services on our behalf. This sharing is covered by agreements to maintain your privacy to the same level as we require of ourselves, and data shared is strictly restricted to that necessary for delivering services.

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards;

The majority of our data is held in the UK and the EEA; some data is held in the United States of America.

- The data held in UK secure data centres under contractual agreements with Sungard AS.
- Much of our cloud provision is provided by Microsoft and this is covered by EU Model Contractual Clauses. This data is stored in the UK and EEA.

The two provisions above cover the majority of our data. For the remainder:

- There are a number of other suppliers providing cloud services to us; these are all covered under contractual agreements within the UK and use UK or EEA storage.
- Some data services are shared with other parts of government and health
- Some services are supplied by US companies which are governed by either use of EU-US Privacy Shield regulations or via binding corporate rules.

(f) where possible, the envisaged time limits for erasure of the different categories of data;

The time limits for our retention of data are documented in our published retention schedule.

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Article 32(1) measures are documented below:

(a) the pseudonymisation and encryption of personal data;

We use encryption where possible for data on end user devices; encryption is always used where electronic data is in transit outside of Enfield Council. We use pseudonymisation within the Council where we require statistical records but no longer require personal data.

Electronic data access by staff is always from devices with encrypted storage; we also encrypt in transit. We implement policies that prevent access to data from devices that are not secured to our requirements. Data is stored in secure datacentres and in secure cloud storage; all of these have been appropriately risk assessed and are subject to ongoing vulnerability management processes.

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

Confidentiality – all systems have role based access control and many are also restricted to access only from Enfield Council managed devices. There are policy and discipline frameworks in place to provide further controls, and access is logged.

Integrity – we regularly review data on our systems and they are subject to audit. There are also additional verification controls on some systems.

Availability / Resilience – there are service level agreements in place for cloud-based services. For on-site services we use methods such as replication of equipment (e.g. redundant power supplies, RAID) where necessary, and protection for power outages such as uninterruptable power supplies.

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

For cloud services this is dependent on the cloud supplier; we have contractual controls regarding backup and restore as required in these contracts. For on-site services we have regular backups which include testing of backups to ensure recoverability.

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Audits are carried out on our systems; backup testing is undertaken. Where risk warrants, external tests such as penetration testing are used.