Comhairle Cathrach na Gaillimhe
Galway City Council

Data Classification Policy

Version 1.2 January 2025

Introduction

This policy sets out the way in which Galway City Council classifies the protections it places on personal data and special categories of personal data that it processes internally. It also provides details about the type of protections in places on personal data and special categories of personal data (personal data) where the data is required to be transferred internally and where it is transferred to a third party externally.

The Council has included in this policy details of whom can access and handle the personal data and the encryption/security protections required for the different types of personal data that the Council processes.

Scope of policy

This policy applies to all the data processed by the Council employees and any third parties that the Council engage with to process personal data on our behalf.

Furthermore, this policy to inform customers of the Council about the steps we take to ensure that their personal data is protected and processed by employees and third parties only where it is necessary to do so and to ensure we provide the best possible services to our customers.

Data Classification		Description of Data	Working Examples of the data	Storing, Accessing & Sharing of the data
Non-personal data	Public	Any non-personal data such as statistics, policy & procedures or any data uploaded and publicly available on the Council's website.	(1) Council meeting minutes (2) Chief Executive orders (3) Annual Reports	Accessible to all members of the public.
Personal data	Public	Any personal data that is required to published or accessed by members of the public.	(1) Planning applications, (2) Grants paid (3) Elected City Councillor's	Accessible to all members of the public.
Personal Data	High	Names, e-mail address, home address and contact numbers of customers	(1) Parking fines (2) Council tenants (3) Housing Assistance Applicants	Only staff processing the data should have access to it. All other staff should be restricted from accessing. Transfers should be encrypted to 3rd parties.

				Internal sharing must obtain informed consent from the customer.
Special Categories of Personal Data	Critical	Health data, disability data, sexual orientation, union membership, racial or ethnic data	(1) Housing grant for those with disabilities. (2) Traveller accommodation data (3) HAP application detailing family make-up (4) Medical reports & disability records for staff & customers.	Only staff processing the data should have access to it. Any paper based data should be securely kept in locked cabinets & a log kept of staff who access the data should be maintained. Digital files of the data should have access restricted to staff within section or only working on the file and the line manager of the section. Internal sharing must have informed consent from customer. Transfer the data to third party requires encryption of the data & 2 art. 9 reasons for sharing must be complied with. Consent must be obtained from the customer.