HARLOW COUNCIL
Data Security Breach Management Policy

Document Information

Policy Author(s):		Document Version No:	
Approved and authorised:		Document Version Date:	
Date authorised:		Document Type:	**Policy**
Service(s)		Department(s)	**Corporate Information and ICT**

1. Introduction

Harlow District Council is registered with the Information Commissioner as a Data Controller – an organisation that processes personal data. All Data Controllers have a responsibility under the Data Protection legislation and General Data Protection Regulation (GDPR) to comply with the requirements of the integrity and confidentiality principle of the GDPR. That is to ensure that the appropriate technical and organisational processes are in place to protect the personal data collected by the Council.

Article 5(1)(f) of the GDPR states that organisations which process personal data must be "Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

No organisation handling personal information can guarantee that it will never experience losses but by ensuring that standards are equivalent to, or exceed, best practice, data subjects will be reassured that all reasonable steps are taken to preserve and protect their information.

There are new mandatory reporting duties on data controllers and processors to notify the ICO of data breaches that pose a risk to the rights or freedoms of data subjects, for example risk of identity theft. Notification should be within 72 hours of becoming aware of the breach or potential breach, failure to notify may result in the Council being subjected to an administrative fine up to 10 million Euros or 2% of global turnover whichever is the higher.

Only in exceptional circumstances can the notification be delayed, written justification must be provided of any delay and the possible consequences of the delay in reporting.

All data breaches must be reported to the Council's Data Protection Officer who is the named contact for the ICO.

The Council has a separate procedure for Council staff to follow when a data breach occurs.

2. Scope of policy

The Council is obliged under Data Protection legislation /GDPR to have in place a framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility which can be found in the Council's Data Breach Reporting Procedure.

Council staff will process personal data as part of their job and will adhere to the Data Protection legislation/GDPR.

3. Policy Statement

All users of personal data within the Council have a responsibility to ensure that they process personal data in accordance with the Data Protection legislation /GDPR and the six Data Protection Principles.

The Principles are that personal data must be processed with:

1. lawfulness, fairness and transparency;
2. purpose limitation;
3. data minimisation, (to only hold the minimum amount of personal data to enable processing);
4. accuracy;
5. storage limitation (not kept for longer than necessary);
6. integrity and confidentiality (that is be securely stored).

The Council will follow the data processing principles above and have the appropriate technical and organisational security measures in place to minimise the risk of breaches of personal information.

The Council will have the necessary contract provisions in place with data processors, contractors who process personal data on behalf of the Council, to ensure compliance with the data protection processing principles, and breach notification duties in the GDPR and Data Protection legislation.

Any employee or member of the public, who has a concern about processing or storage of personal information, is urged to contact the Data Protection Officer.

The Data Protection Officer details are:

Data Protection Officer
The Civic Centre
The Water Gardens
Harlow
CM20 1WG
data.protection@harlow.gov.uk