DATA BREACH POLICY

V.1 26 August 2021

Governance Legal Services

Review Date 25 August 2022

Inward Facing Policy

Introduction

Harlow District Council (Council) is registered with the Information Commissioner (ICO) as a Data Controller – an organisation that processes personal data. All Data Controllers have a responsibility under the Data Protection Act 2018 (DPA) to comply with the requirements of Principle 7.

The UK General Data Protection Regulations (UK GDPR) requires the Council to have in place appropriate technical and organisational measures to implement the Principles and safeguard individuals rights. The Council has a legal requirement to integrate data protection into all processing activities and business practices, being "privacy by design".

Principle 7 of the DPA requires that the Council be responsible for and be accountable to processing data and treat data "in a manner that ensures appropriate security ……, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to , personal data. This includes breaches that are both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Common breaches include sending an email to the wrong recipient, incorrect use of addresses when posting letters, and allow long email trails to be shared widely.

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. This Policy provides a framework to be followed by all Council employees for avoiding, reporting, and investigating any breaches of the DPA.

A data breach can occur for a variety of reasons, for example:

a) Human error
b) Unforeseen circumstances such as a fire or flood
c) Hacking attack on the Council's ICT systems
d) 'Blagging' offences where information is obtained by deceit
e) Loss of paper records
f) Loss or theft of data or equipment on which data is stored
g) Inappropriate access controls allowing unauthorised use
h) Equipment failure

Purpose Statement

The Council is obliged under DPA to have in place a framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

Council staff will process personal data as part of their job and must adhere to the DPA. A breach may result in the Council being liable in law for the consequences of the breach.

The objectives of this Policy are to:

(i) Detail the steps to take following a breach
(ii) contain any breaches of the DPA,
(iii) to minimise the risks associated with the breach
(iv) consider what action is necessary to secure personal data and prevent further breaches.

This Policy is based on guidance issued by the Information Commissioner's Office (ICO).

Policy Statement

All users of personal data within the Council have a responsibility to ensure that they process such data in accordance with the DPA and the Data Protection Principles (Principles).

The Principles are that personal data must be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) 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 ('integrity and confidentiality').

Data Breach

Any data breach arising within the Council could constitute an offence.

Certain offences may be treated extremely seriously and may also constitute breach of Officer Codes of Conduct engaging disciplinary procedures, up to and including dismissal. Any employee, who has a concern about processing or storing personal information, is urged to contact admin.legal@harlow.gov.uk to obtain advice and support.

All breaches, for example unauthorised or unlawful processing or accidental loss, must be reported **immediately** so that the appropriate measures can be taken to limit the damage to the individual or individuals and to protect the Council from loss of public confidence. The Council is required to report certain breaches to the ICO within 72 hours of the breach.

Reporting a Data Breach

A data breach form is available on Kaonet.

The form will ask you for the following information:

- Reporting Officer Name, Department, Extension Number, Email address
- Please describe what happened to result in a data breach
- Please describe what immediate actions you have taken following discovery of the breach (including containing the breach, and advising the data subjects of the breach)
- Number of data subjects affected
- Type of Data Subject [a drop list will be provided to assist with selection]
- Potential consequences of the breach
- Please give full details of how the incident occurred
- How did the breach come to your attention?
- Please give full details of all preventative measures your department has in place to avoid data breaches
- Date of actual Breach
- Time of actual Breach
- Date when the Breach came to your attention
- Time when the Breach came to your attention
- Please indicate ALL of the data categories included in the breach (drop down)
- Please give full details of step you will take to prevent a recurrence and when these steps will be completed.
- Please confirm the last date of GDPR training for all officers involved with the breach

If the breach is discovered outside normal working hours, this should begin as soon as is practicable.

Actions Taken Following a Breach

Third Tier Manages will assist with a review of the data breach to understand how and why it occurred, and what steps the Council will need to take to prevent recurrence which may include:

- Ensuring there are appropriate checking and verification measures in place with regards to sending personal data;

- Highlighting the importance of double checking information within staff data protection training as this will aid in imbedding data protection awareness in their daily tasks. Refresher training should be provided when needed;

- Use of ICO Resources to help with on-going training – which should be refreshed yearly;

- Password protecting information which contains personal data;

- Timely implementation of any remedial measures identified, supported with sufficient practical guidance concerning the changes made as a result of the breach;

- Ensuring appropriate action is taken if further information comes to light which impacts the affected data subject;

- Ensuring that existing preventative measures are followed routinely and consistently.

Governance

The Chief Executive has overall accountability for implementing this Policy within the Council. This responsibility may be delegated to Head of Governance and the appointed Data Protection Officer (DPO).