MACCLESFIELD TOWN COUNCIL

PERSONAL DATA BREACH POLICY

DOCUMENT VERSION CONTROL

Document Title: PD Breach Policy

Version No.	Date Change Made	New Version No.	Changes Made By (initial)	Comment
00.01	May 2018		HW	New policy for GDPR

Table of Contents

Introduction

This document is an integral part of demonstrating GDPR compliance to ensure personal data breaches are addressed properly, appropriately and in a timely manner.

This policy has been produced in response to GDPR Article 33 – "Notification of a personal data breach to the supervisory authority" – and GDPR Article 34 of the GDPR – "Communication of a personal data breach to the data subject".

A breach of GDPR affecting the rights and freedoms of individuals can result in a financial penalty (up to 20 million euros).

Failure to report a breach can result in a fine of up to 10 million euros.

Macclesfield Town Council will be legally responsible for personal data breaches.

What is a personal data breach?

The UK Information Commissioner's Office (ICO) defines a personal data breach as:

> "A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

There are three breach notification obligations:

- Data processor to notify data controller
- Data controller to notify their Supervisory Authority (for the UK this is the ICO)
- Data controller to notify the data subject

Reporting an incident

Any Councillor or Officer (or data processor) who becomes aware of a breach must report it immediately to the Clerk.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is possible.

The Clerk will complete will enter the details into the Personal Data Breach Form and inform the Data Protection Officer (DPO).

Incident investigation, containment and recovery

The DPO will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the DPO in liaison with Clerk to establish the severity of the breach.

The DPO and Clerk will:

- Investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur. The investigation will need to take into account the following:
  - the type of data involved;
  - its sensitivity;
  - the protections that are in place (e.g. encryptions);
  - what has happened to the data (e.g. has it been lost or stolen);
  - whether the data could be put to any illegal or inappropriate use;
  - data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);
  - whether there are wider consequences to the breach.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms.
- Establish whether there is anything that can be done to recover the personal data and limit the damage the breach could cause.
- Establish who may need to be notified as part of the initial containment.
- Determine the suitable course of action to be taken to ensure a resolution to the incident.

A record will be kept of any personal data breach, regardless of whether notification was required.

Reporting the incident to the ICO

The DPO will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of when the breach was first detected.

Every incident will be assessed on a case by case basis. However, the ICO must be notified if the breach:

- Is likely to result in a risk to the rights and freedoms of the individuals;

- Will result in a risk of damage to reputation, financial implications, confidentially loss, and discrimination, social and economic disadvantages that may occur to the concerned individual.

The following information must be provided to the ICO:

- The categories and approximate number of individuals concerned;
- The categories and approximate number of personal data records concerned;
- The name and details of the DPO;
- A description of the likely consequences of the personal data breach;
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and where appropriate of the measures taken to mitigate any possible adverse effects.

Breaches can be reported to the ICO via their website.

Notifying the affected individuals

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay.

Notification will include:

- A description of how and when the breach occurred and the data involved;
- Specific and clear advice will be given on what the individual(s) can do to protect themselves;
- What action has already been taken to mitigate the risks;
- The contact details of the DPO;
- Contact details for Macclesfield Town Council for further information or to ask questions on what has occurred.

Evaluation and response

Once the incident has been contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- where and how personal data is held and where and how it is stored;
- where the biggest risks lie including identifying potential weak points within existing security measures;
- whether methods of transmission are secure, sharing minimum amount of data necessary;
- staff awareness;
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

The DPO will keep a record of all data breaches, comprising of the facts, effects and remedial actions

Rehearsal of the incident response procedure

The Clerk and DPO will, at least once year, rehearse the personal data breach procedure through a scenario in which a personal data breach has occurred. The purpose of this is to ensure the response is effectual.

Following the conclusion of the rehearsal the DPO and Clerk will hold a debrief.

The breach response procedure will be revised and reissued it if necessary.

Councillors and officer will be informed of any changes to the procedure.

Annex: Recital 33

Notification of a personal data breach to the supervisory authority.

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

a) Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) Describe the likely consequences of the personal data breach;
d) Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Annex: Recital 34

GDPR Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

a) A the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b) B the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
c) C it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.