Data Breach and Information Security Incident Policy

1.0 Introduction

1.1 The Parish Council utilises various information systems and holds data / information which may include personal or confidential information (about people), and also non-personal information which could be sensitive or commercial, for instance financial data.

1.2 Care should be taken to protect these information assets from incidents (either accidentally or deliberately) that could compromise their security.

1.3 In the event of a data breach or an information security incident, it is vital that appropriate actions are taken to minimise associated risks

2.0 Purpose

The purpose of this policy is to set out the procedure that should be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents within the Parish Council.

3.0 Scope

This policy applies to all Council staff, Councillors, contractors and third party agents handling Parish Council information assets.

4.0 Responsibilities

4.1 All users of Parish Council information assets are required to familiarise themselves and comply with this policy.

4.2 All individuals who access, use or manage the Parish Councils information are responsible for reporting data breach and information security incidents immediately to the DPO (Data Protection Officer) dpo@rayne-essex.gov.uk

5.0 Definition of an incident

An incident in the context of this policy is an event which has caused or has the potential to cause damage to the Parish Councils information assets or reputation. Examples are:

- Accidental loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick)

- Unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)

- Unauthorised disclosure of sensitive or confidential information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee)

- Compromised user account (e.g. accidental disclosure of user login details through phishing)

- Failed or successful attempts to gain unauthorised access to Parish Council information or information systems

- Equipment failure

- Malware infection

- Disruption to or denial of IT services

6.0 Action to be taken in the event of a data breach

On discovery of a data breach the following actions should be taken:-

- Containment and recovery

- Assessing the risk

- Notification of the breach to the Parish Council DPO at dpo@rayne-essex.gov.uk who will inform the Information Commissioner's Office (ICO)

- Evaluation and response

7.0 Containment and recovery. Who is responsible for action?

The individual committing the breach, the individual finding the breach

8.0 Action to be taken

The immediate priority is to contain the breach and limit its scope and impact.

Where personal data has been sent to someone not authorised to see it staff/councillors should:

- tell the recipient not to pass it on or discuss it with anyone else;

- tell the recipient to destroy or delete the personal data they have received and get them to confirm in writing that they have done so;

- warn the recipient of any implications if they further disclose the data; and

- inform the data subjects whose personal data is involved what has happened so that they can take any necessary action to protect themselves.

9.0 The DPO must be notified at dpo@rayne-essex.gov.uk and the following information must be provided:

- date and time of the breach;

- date and time breach detected;

- who committed the breach;

- details of the breach;

- number of data subjects involved; and

- details of actions already taken in relation to the containment and recovery.

10.0 Assessing the risk .

Who is responsible for action? The Parish Council's DPO.

Action to be taken:

The Parish Councils DPO will conduct an investigation into the breach and prepare a report. This report will follow the ICO's guidance on Breach Management and will consider the following:

- How the breach occurred.
- The type of personal data involved.
- The number of data subjects affected by the breach.
- Who the data subjects are.
- The sensitivity of the data breached.
- What harm to the data subjects can arise? For example, are there risks to physical safety, reputation or financial loss?
- What could happen if the personal data is used inappropriately or illegally?
- For personal data that has been lost or stolen, are there any protections in place such as encryption?
- Are there reputational risks from a loss of public confidence in the service the Parish Council provides?

11.0 Notifying the Information Commissioner. Who is responsible for action?

The Parish Council DPO is responsible for notifying the ICO **within 72 hours**.

12.0 Evaluation and response

Once the breach has been dealt with, the cause of the breach needs to be considered. There may be a need to update policies and procedures, or to conduct additional training.

Date Effective From: March 2018

Last Review Date: May 2019

Next Review Date: May 2020