

# Hutton Henry and Station Town Parish Council

## Data Breach Policy & Reporting Form

Adopted July 2023

This policy specifies the actions with respect to breaches of personal data.

### What is a breach?

A data security breach can happen for several reasons: Loss or theft of data or equipment on which data is Stored, Inappropriate access controls allowing unauthorised use, Equipment failure, Human error, Unforeseen circumstances such as a fire or flood, Hacking attack, 'Blagging' offences where information is obtained by deceiving the organisation who holds it. This policy and form (see appendix A) will be used to report such breaches.

### What is Personal Data?

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 the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example - Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and loss of availability of personal data
- Reportable theft or loss of an unencrypted laptop computer or other unencrypted portable electronic/digital media holding names, addresses, dates of birth and National Insurance Numbers of individuals.
- A manual paper-based filing system (or unencrypted digital media) holding the personal data relating to named individuals and their financial records etc.

More information can be found using the below link:

[https://ico.org.uk/media/fororganisations/documents/1562/guidance\\_on\\_data\\_security\\_breach\\_management.pdf](https://ico.org.uk/media/fororganisations/documents/1562/guidance_on_data_security_breach_management.pdf)

### Breach Containment and Recovery Article 2(2) of the Notification Regulation states:

The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible. The provider shall include in its notification to the competent national authority the information set out in Annex I. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by telephone, fax, email, text and picture or video message, or by using an automated calling system. PECR also include other rules relating to cookies, telephone directories, traffic data, location data and security breaches. Detection of a personal data breach shall be deemed to have taken place when the provider has acquired sufficient awareness that a security incident has occurred that led to personal data being compromised, to make a meaningful notification as required under this Regulation.

# Hutton Henry and Station Town Parish Council

## Dealing with an incident - Reporting Point

On discovery of an incident either because of automatic notification, accidental discovery, manual record checking or any other means, all personnel shall;

1. Report the incident via email to the reporting points (clerk of the council and chairman).
2. The email report should be followed by a telephone call to the clerk or council chairman.
3. Should neither the clerk nor the chair be available the vice-chair of the council should be informed.
4. Should the vice-chair not be available all members should be notified via email.

## Reporting Point Responsibilities

All incidents must be recorded. The reporting point shall perform the following actions;

- Note the time, date and nature of incident together with a description and as much detail as appropriate on an Incident Response Form (see appendix A)
- Ensure the protection of any evidence and that a documented chain of evidence is maintained.
- Liaise with relevant authorities, individuals and the media where appropriate.
- Keep a note of all communications together with their date, time, who has been communicated with, and what the content and nature of communication was on the Incident Response Form.

### 1. Incident Response Plan

Assess the risk to individuals because of a breach: The following must be considered:

- the categories and approximate number of individuals concerned, and;
- the categories and approximate number of personal data records concerned, and;
- the likely consequences of the personal data breach, consider if the impact results in a risk to the rights and freedoms of individuals.
- To help assess the risks refer to the Information Commissioner Office (ICO) website:
  - a. <https://ico.org.uk/for-organisations/report-a-breach/>
  - b. <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

### 2. If the incident is deemed to be a notifiable incident the following actions must be taken:

a) Within 72 hours of becoming aware of the incident (even if not aware of all the details yet):

b) Call ICO: 0303 123 1113 – and provide the following information:

- what has happened;
- when and how the council found out about the breach;
- the people (how many) that have been or may be affected by the breach;
- what the council are doing as a result of the breach; and
- who else has been told.

c) For reporting a breach outside normal working hours use the ICO Reporting Form:

<https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>

## Hutton Henry and Station Town Parish Council

### **3. If the incident is deemed to result in a high risk to the right and freedoms of individuals:**

a) Within 48 hours the affected individuals must be informed by telephone, letter or email about the incident as there may be a need for them to take actions to mitigate immediate risk of damage to them.

b) The individuals must be told in clear and plain language:

- (i) the nature of the personal data breach and;
- (ii) A description of the likely consequences of the personal data breach; and
- (iii) A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects, and;
- (iv) The name and contact details of the clerk and chairman from where more information can be obtained;

### **4. If the incident is not deemed to be notifiable:**

a) Update the Security Incident Log form (Appendix B)

b) Include the steps and evidence used to identify and classify the risk. Include reasons why the incident is not deemed to result in a risk to the rights and freedoms of individuals.

### **5. Incident Review**

The council clerk and chairman will ensure that the incident is reviewed at the next appropriate Council meeting under the Policy and Security section of the agenda.

a) The Council will consider whether discussion of the incident warrants exclusion of the press and public from the meeting during that discussion.

b) At that meeting the council should determine if there are any further actions that need to be assigned or completed because of the incident.

c) It should be noted that this final stage of the incident may require a review of this policy document.

# Hutton Henry and Station Town Parish Council

## Appendix A – Data Breach Reporting Form

<b>Date &amp; Time of notification of breach</b>	
<b>Notification of breach and to whom</b> Name & Contact Details	
<b>Details of breach</b>	
<b>Nature and Content of Data involved</b>	
<b>Number of individuals effected</b>	
<b>Name of person investigating breach</b> Name Job Title Contact Details Email Phone Number Address	
<b>Information Commissioner informed</b> Time and method of contact <a href="https://report.ico.org.uk/security-breach">https://report.ico.org.uk/security-breach</a>	
<b>Police Informed if relevant</b> Time and method of contact Name of person contacted Contact details	
<b>Individuals contacted</b> How many individuals contacted? Method of contact used to contact?	
<b>Does the breach affect individuals in other EU member states?</b> <b>What are the potential consequences and adverse effects on those individuals?</b> Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of taking those measures is relayed to the individuals involved.	
<b>Staff Briefed</b>	
<b>Assessment of ongoing risk</b>	
<b>Containment Actions: technical and organisational security measures have you applied (or were to be applied) to the affected personal data</b>	
<b>Recovery Plan</b>	
<b>Evaluation and response</b>	

## Hutton Henry and Station Town Parish Council

### Appendix B Security Incident Record Form

<b>Date of Incident</b>	<b>Risk Identification and Classification</b> Include the steps and evidence used to identify and classify the risk	<b>Incident Review Details: Meeting</b> Record the actions taken to report the breach; the meeting date and actions taken because of the breach	<b>Name and Signature</b> Officer investigating breach