Horley Town Council
Data Breach Policy

1. Introduction:

What is a Data Breach?

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.

2. Background:

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

3. Dealing with a Data Breach

3.1 On discovery of an incident either as a result of automatic notification, accidental discovery, manual record checking or any other means, all personnel or Councillors shall;

a) Report the incident by email to the Chief Executive Officer of the Council at: Info@horleysurrey-tc.gov.uk

b) The email report should be followed by a telephone call to the Chief Executive Officer who will then notify the Council Chairman or, in their absence, the Vice-Chairman.

3.2 All incidents must be clearly documented by the Chief Executive Officer and the following actions taken:

- Details of the time, date and nature of incident together with a description and as much detail as appropriate on an Incident Response Form.

- 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.

4. Incident Response Plan

4.1 To assess the risk to individuals as a result of a breach, the following must be considered:

a. the categories and approximate number of individuals concerned;

b. the categories and approximate number of personal data records concerned, and;

c. the likely consequences of the personal data breach, in particular, a potential risk to the rights and freedoms of individuals.

d. The Information Commissioners Office (ICO) may be contacted for further guidance at: https://ico.org.uk/for-organisations/report-a-breach/

4.2. 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, contact the ICO at : 0303 123 1113 and provide the following information:

- what has happened;
- when and how the Council found out about the breach;
- how many individuals have been or may be affected by the breach;
- what the Council is doing as a result of the breach; and
- advise who will be the main contact for this incident will be at the Council (ie. the Chief Executive Officer).

b. For reporting a breach outside normal working hours use the ICO Reporting Form:

https://ico.org.uk/for-organisations/report-a-breach/

4.3 If the incident is deemed to result in a high risk to the right and freedoms of individuals:

(Examples include but are not limited to a ransomware attack which results in the Council's personal data being encrypted and data can't be restored; a HR file left on bus; unencrypted personal data is emailed to Councillor and his emails are hacked). The following action must be taken:

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

- the nature of the personal data breach
- 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 including, where appropriate, the measures taken to mitigate any possible adverse effects
- the name and contact details of the Chief Executive Officer from where more information can be obtained

c. **However,** if the following can be demonstrated, then the Chief Executive Officer/Chair **does not** need to communicate with the individual:

- The Council has implemented appropriate technical and organisational measures that have rendered the personal data unintelligible to any person who is not authorised to access it, such as encryption
- The Council has taken subsequent measures that ensure the high risk to the rights and freedoms individual is no longer likely to materialise or
- Would involve a disproportionate effort. In such an instance a public communication should be made.

4.4 If the incident is not deemed to be notifiable:

a. Update the Incident Response Form along with the outcome of the risk assessment.

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 Chief Executive Officer will ensure that the incident is reviewed at the next Full Council meeting and preventative measures considered to avoid any recurrence.

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 shall determine if there are any further actions that need to be assigned or completed as a result of the incident.

c. The Council may consider referring further actions and to a committee, working group or external parties.

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

6. Data processors duty to inform Horley Town Council

If a data processor, legitimately processing personal data on behalf of Horley Town Council, becomes aware of a personal data breach, it must notify the Chief Executive Officer, without undue delay. The Chief Executive Officer will then act on the Council's behalf and inform the ICO. It is not the data processor's responsibility to notify the ICO.

Data Security Breach Reporting Form

A data security breach can happen for a number of 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. Use this form to report such breaches.

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 l. 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, in order to make a meaningful notification as required under this Regulation.

Date and time of Breach notification	
Notification of breach to whom Name Contact details	
Details of breach	

Nature and content of data involved	
Number of individuals affected	
Details of person investigating Name Job Title Email Address	
Information Commissioner informed? Time & Method of contact https://report.ico.org.uk/security-breach/	
Police informed (if relevant) ? Time & Method of contact Name of person contacted Contact details	
Individuals contacted How many people contacted? Method of contact used? Does the breach affect individuals in other EU member states? What are the potential consequences and adverse effects on those individuals?	

Confirm that details of the nature of the risk to the individuals affected: - Any measures they can take to safeguard against it - Likely cost to them of taking those measures is relayed to the individuals involved	
Staff Briefed Names & dates	
Assessment of ongoing risk	
Containment Actions: technical and organisational security measures you have applied (or were to be applied) to the affected personal data	
Recovery Plan	
Evaluation and response	