Kingsteignton Town Council

Breach Notification Policy

1. Introduction

1.1 Under the terms of the GDPR Kingsteignton Town Council is obliged to report any breach of data security. The terms of this policy covers the scope, and method of such reporting, and what further actions need to be taken

2. Scope

2.1 The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. Kingsteignton Town Council must do this within 72 hours of becoming aware of the breach, where feasible.

2.2 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Council must also inform those individuals without undue delay.

2.3 The Council ensures that there is robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not the Council needs to notify the relevant supervisory authority and the affected individuals.

2.4 The Council must also keep a record of any personal data breaches, regardless of whether you are required to notify.

3 Identification

3.1 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.

3.2 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.

3.3 When a personal data breach has occurred, the likelihood and severity of the resulting risk to people's rights and freedoms needs to be established. If it's likely that there will be a risk then the procedure to report the breach must be used. If it's unlikely that there is a risk to rights and freedoms, then the breach must be recorded, and must include a justification of the decision.

3.4 In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR identifies more than the usual harms.

4 Data Processors/3rd Parties

4.1 The Council uses several data processors/3rd Parties, and if any of these processors suffers a breach, then under Article 33(2) it must inform the Council without undue delay as soon as it becomes aware. The requirements on breach reporting should be detailed in the contract between the Council and the processor/3rd Party, as required under Article 28.

5 Timing

5.1 The Council must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. There must be a justification if this is not done within the timescale.

6 Breach Information

6.1 When reporting a breach, the Council has to provide the following information:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

6.2 Failing to notify a breach when required to do so can result in a significant fine, and can be combined with the ICO's other corrective powers under Article 58.

6.3 Serious breaches should be reported to the ICO using the DPA security breach helpline on 0303 123 1113 or in writing by using the DPA security breach notification form, which should be sent to the email address casework@ico.org.uk or by post to the ICO office address Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Further advice will be given at that point.

The security breach notification form can be found here:

https://ico.org.uk/media/fororganisations/documents/2666/security_breach_notification_form.doc

7. Informing Individuals

7.1 If a breach is likely to result in a high risk to the rights and freedoms of individuals, the Council must inform those concerned directly and without undue delay.

7.2 The definition of 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. An assessment will need to be made regarding both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring, a higher risk means there is a greater possibility of damage or harm to the individuals.

7.3 Details required to be passed to affected individuals are:

- the name and contact details of the Council's data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- 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.

8. Other steps

8.1 The Council should ensure that all breaches, regardless of whether or not they need to be reported to the ICO are recorded.

8.2 Article 33(5) requires the Council to document the facts relating to the breach, its effects and the remedial action taken. This covers the Council's obligation to comply with the accountability principle and enables verification of compliance of the Council's notification duties.

Breach Notification Form

Council Name:	**Kingsteignton Town Council**

Reference Number of Incident	
Date Incident Detected	
Date Incident Occurred	
Name of Incident Owner	
Details of Incident	
Personal/Sensitive Data?	
Manual/Automated Data?	
Encrypted Data?	
Volume of Data	
Notification Date	
Notification Reference	
Extra Information	