Data Breach Process

Although Crudwell Parish Council takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen.

Examples of data breaches include:

• Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone)
• Inappropriate access controls allowing unauthorised use
• Equipment failure
• Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space)
• Unforeseen circumstances such as fire or flood
• Hacking attack
• 'Blagging' offences where information is obtained by deceiving the council.

However if a breach has occurred, the following steps should be taken immediately:

1. Internal Notification: Individual who has identified the breach has occurred must notify the Clerk. A record of the breach should be created using templates kept on file as follows:

a. Data Breach Incident Form
b. Data Breach Log
c. Evidence Log

However, the information that must be provided must include;

• Contact name and number of person reporting the incident
• The type of data or information involved
• Whether the loss of the data puts any person or other data at risk
• Location of the incident
• Inventory numbers of any equipment affected
• Date and time the security incident occurred
• Location of data or equipment affected
• Type and circumstances of the incident

The Chairman of the Council must also be informed to enable he/she to confirm that the details represent a valid breach as defined above. The outcome of these actions are to be reported to the Parish Council for information and to be recorded or actioned as legislation dictates.

2. Containment: the Clerk to identify any steps that can be taken to contain the data breach (e.g. isolating or closing the compromised section of network, finding a lost piece of equipment, changing access codes) and liaise with the appropriate parties to action these.

3. Recovery: the Clerk to establish whether any steps can be taken to recover any losses and limit the damage the breach could cause (e.g. physical recovery of equipment, back up tapes to restore lost or damaged data)

4. Assess the risks: Before deciding on the next course of action, the Clerk will assess the risks associated with the data breach giving consideration to the following, which should be recorded in the Data Breach Notification form:

a. What type of data is involved
b. How sensitive is it?
c. If data has been lost/stolen, are there any protections in place such as encryption?
d. What has happened to the data?
e. What could the data tell a third party about the individual?
f. How many individuals data have been affected by the breach?
g. Whose data has been breached?
h. What harm can come to those individuals?
i. Are there wider consequences to consider such as reputational loss?

5. Notification to the Information Commissioners Office (ICO): Following the risk assessment in step 4, the Clerk should notify the ICO within 72 hours of the identification of a data breach if it is deemed that the breach is likely to have a significant detrimental effect on individuals. This might include if the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social disadvantage.

The Clerk should contact ICO using their security breach helpline on 0303 123 1113, option 3 (open Monday to Friday 9am-5pm) or the ICO Data Breach Notification form can be completed and emailed to casework@ico.org.uk.

6. Notification to the Individual: The Clerk must assess whether it is appropriate to notify the individual(s) whose data has been breached. If it is determined that the breach is likely to result in a high risk to the rights and freedoms of the individual(s) then they must be notified by the parish council.

7. Evaluation: The Clerk/ Council should assess whether any changes need to be made to their processes and procedures to ensure that a similar breach does not occur.

This policy will be reviewed on an annual basis at the Parish Councils December meeting each year.

The policy may also be reviewed if legislation changes or if monitoring information suggests that policy or practices should be altered

Created: Dec 2022

Revised: N/A

Adopted: 20/12/2022

Next review: Annually – December Parish Council meeting