Combs Parish Council Data Breach Policy & Procedure

The intention of this policy and procedure is to give Combs Parish Council a systematic response to any reported data breach and ensure that it acts in a responsible manner managing and protecting the personal data which it holds in accordance with the law.

All breaches will be investigated and recorded in a timely manner to ensure any necessary actions may be taken to rectify the breach and prevent any further damage.

• the ICO and data subjects will be informed as required in more serious cases
• incidents will be reviewed, and lessons learned from these

Combs Parish Council uses Article 4 (12) of the General data protection Regulation ("GDPR") which defines a data breach as:

"A breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

Combs Parish Council is obliged under the GDPR to act in respect of such data breaches outlined in Article 4 (12)

This procedure sets out how the Council will correctly investigate and manage any reported breach conforming with any time frame required by law,all breaches will be reported if necessary to the data subjects and I.C.O. with remedial action taken to rectify the breach.

On Discovery of A Breach

Suspected data security breaches should be reported promptly to the Clerk and Chairman as the primary points of contact.

The report must contain full and accurate details of the incident using the following as a guide:

Reported by:

Summary of Breach:
(Who,What,When)

Specific Document Details:
(Document Titles,contact details,Financial etc.)

Upon receipt of this the Clerk and Chairman will action the report either on their own volition or convene a full council E.G.M. as they see necessary but all within any legal time constraints.

They will,

Report their actions taken as recipients of the data breach report:
This will be reported to the full council (The I.C.O. and any involved data subjects as necessary)

Report what action has been taken to retrieve any data and close the breach:

Report any individual involved with the data breach and any appropriate action taken.
(Training etc.)

Detail any breach notification to the data subjects involved:
(Note any support offered)

Conclusion:
(This should include any lessons learned, any changes required to prevent further data losses, any further training requirements)

Article 33 of the GDPR requires the Council as data controller to notify the ICO only when the breach "is likely to result in a risk to the freedoms and rights of natural persons". Such a breach also must be communicated to the data subject (with certain exceptions). Notification must be made "without undue delay" and within 72 hours of becoming aware of it. If the Council fails to do this, it must explain the reason for the delay.
Article 33(5) requires that the Council must maintain documentation on data breaches, their nature and remedial action taken.

A report to the ICO must contain information as to the nature of the breach, categories of data,, number of data records, number of people affected, name and contact details of likely consequences of the breach and action taken.

The Parish Council's response to any reported data security breach will involve the following:

Containment and Recovery
Assessment of the Risks
Consideration of Further Notification
Evaluation and Response

This document shall be subject to annual review by the full Combs Parish Council

Further information may be found at:

www.ico.org.uk

www.gdpr-info.eu

Approved at the council meeting on 9 May 2023