



# ECCLESFIELD PARISH COUNCIL

*Serving the Community since 1894*

## **SECURITY INCIDENT POLICY**

### **Introduction**

All Data Controllers (Ecclesfield Parish Council) have a responsibility under the Data Protection Act 2018 (DPA) to ensure appropriate and proportionate security of the personal data they hold.

The DPA states that 'appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'.

Planning for a breach is therefore essential; every council should have a breach response plan, and should designate, in advance the committee or officer to deal with such an incident.

### **Ecclesfield Parish Council would**

- Identify the designated committee or officer who is notified if there is a breach
- Identify the designated committee or officer who would manage and determine whether a personal breach of data has occurred
- Investigate the breach (this may be designated to the committee or an officer)
- The committee or officer would be provided with delegated power to make the final decision on behalf of Ecclesfield Parish Council

### **What is a breach – identifying whether a breach has occurred**

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.

Personal data breaches can include

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction by the data controller or processor (officer of the council))
- 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

## **Breach Response Plan**

- The response plan would include assessing the risk to individuals as a result of a breach.
- Should a breach occur then the Information Commissioners Office (ICO) should be notified within 72 hours of becoming aware of the breach (even if the Parish Council are not aware of all the details of the breach within the 72 hours)
- Ensure the committee or officer is aware of all the information it must provide to the ICO about the breach

## **What should be provided to the ICO**

The Committee or Officer would endeavour to provide a description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the Parish Councils point of contact where information can be obtained;
- 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, including, where appropriate, the measures taken to mitigate any possible adverse effects;
- Explanation of what has happened;
- When and how the breach was found;
- The people that may be affected by the breach and how many people are affected; and
- What the Parish Council is doing as a result of the breach

The ICO can be contacted on 0303123113

## **Notifying those affected by the breach**

The Parish Council would inform the affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms in accordance with the GDPR without undue delay.

The information provided to an individual would include

- A description, in clear plain language, the nature of the personal data breach
- The name and contact details of the committee or officer where more information could be obtained
- A description of the likely consequences of the personal data break; and
- A description of the measures the Parish Council would take to deal with the personal data breach, including the measures to mitigate risks in the future

The Parish Council would record every personal data breach even if they are not reported to the ICO and inform the insurance provider.

The Parish Council would review the technical and organisational measures for the security of personal data within the Parish Council and implement changes required to minimise the risk of such breaches reoccurring.

**Approved by Council 9.1.2020**

**Review date November 2022**