Acaster Malbis Parish Council

e: parish.clerk@acastermalbis-pc.gov.uk
w: www.acastermalbis-pc.gov.uk

DATA BREACH POLICY

1 Introduction

Acaster Malbis Parish Council holds a large amount of information in a variety of formats stored on computers, in written documents, printed documents and photographs. This may include personal, sensitive or commercially confidential data.

The council has a legal duty to safeguard information in its control and so care should be taken to protect information, to ensure its integrity and to protect it from loss, theft or unauthorised access.

However, in the event of a data breach, it is important that the council acts quickly and appropriate action is taken to minimise associated risks, and to comply with its legal responsibilities.

2 Scope

This document applies to all councillors, employees of the council, contractual third parties and agents of the council who have access to information systems or information used for council purposes.

3 What is a data beach?

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 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.

4 Incident Response Plan

The incident response plan of the council comprises a number of clearly identifiable steps:

- Report of the incident.
- Forming a Response Team from an initial assessment.
- Containment and recovery.
- Investigation and risk assessment.
- Notification.
- Review.

Each of the above steps are described in more detail below.

5 Reporting of an incident

All incidents will be recorded in the security incident log maintained by the clerk over the lifecycle of the incident.

5.1 To whom?

On discovery of an incident either as a result of automatic notification, accidental discovery, manual record checking or any other means, all personnel shall report the incident to the clerk to the council – parish.clerk@acastermalbis-pc.gov.uk.

5.2 Details required

The clerk will require the person reporting the incident to provide further information, the nature of which will be dependent upon the incident being reported.

In all cases the following information will be requried:

- Contact details of the person reporting the breach.
- The type of data or information involved (not the data unless specifically requested).
- Whether the data relates to people and if so how many people were involved.
- Location of the incident.
- Inventory and location of any equipment affected.
- Date and time the security incident occurred.
- Type and circumstances of the incident.

6 Response Team

A preliminary assessment of the incident will be carried out by the clerk. The chair and clerk will consider the initial assessment and form a response team.

The response team will be the clerk for the smallest data breaches and the clerk and two council members for more significant incidents.

7 Containment and recovery

The response team will determine the appropriate course of action and the required resources needed to limit the impact of the breach. For instance, this may require alerting relevant groups, organisations, parishioners, contractors or suppliers, changing access codes or locks or shutting down critical equipment.

Appropriate steps will be taken to recover data losses. This might entail using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

If there is suspicion that the incident my be criminal in nature, all efforts will be made to preserve evidence integrity.

8 Investigation and risk assessment

An investigation will be undertaken as soon as reasonably possible, but within 24 hours of the data breach being reported.

The investigation will focus on the cause of the breach, the risks associated with it, and will take into account:

- the type of personal data involved;
- the sensitivity of the data;
- the protections in place (e.g. encryptions);

- what happened to the data, whether it has been lost or stolen;
- whether the data can be put to any illegal or inappropriate use;
- the affected individuals, and the potential adverse consequences to them (including how serious/substantial these consequences could be, and the likelihood of occurrence);
- whether there are wider consequences to the breach; and
- other relevant considerations.

9 Notification

9.1 Those affected

The response team will determine if the incident presents a high risk to the rights and freedoms of individuals. If the risk is determined as high:

1. Within 48 hours the affected individuals must be informed about the incident as there may be a need for them to take actions to mitigate immediate risk of damage to them.
2. The individuals must be told in clear and plain language:
    i. The nature of the personal data breach and;
    ii. A description of the likely consequences of the personal data breach; and
    iii. 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, and;
    iv. The name and contact details of the clerk and chairman from where more information can be obtained;

9.2 Information Commissioners Office (ICO)

The response team will determine whether the incident is notifiable to the ICO. A notifiable incident must be reported to the ICO within 72 hours of the initial report.

There is a self-assessment tool on the ICO website to determine if the data breach needs to be reported.

If the data breach is required to be reported the following information will be requested:

- what has happened;
- when and how you found out about the breach;
- the people that have been or may be affected by the breach;
- what you are doing as a result of the breach;
- who we should contact if we need more information and who else you have told.

The information provided should be accurate and with as much detail as possible – a copy of the supplied information will be returned.

10 Review

Once the incident has been contained and any notifications have been made, the response team will carry out a review of the incident.

The review will provide a report to the council with its recommendations such as:

- policy or procedural changes;
- further training;
- additional IT security measures;
- other improvements.