Sandford St Martin Parish Council Security Incident Response Policy

Approved by Sandford St Martin Parish Council on 16 September 2021
Last approved on 05 October 2023

The Security Incident Response Policy links to the Council's Data Protection Policy. This policy must be adhered to in the event of a known or suspected data breach.

What is a breach?
A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or, 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.

Examples of 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
- Loss of availability of personal data.

Dealing with an incident
On discovery of an incident, either as a result of automatic notification, accidental discovery, manual record checking or any other means, the incident must be reported by email to the "reporting points".

Sandford St Martin's reporting points are:

1. Clerk of the Council email to: clerk@sandfordstmartin.org.uk
2. Chairman of the Council email to: jrowe@sandfordstmartin.org.uk

The email report should be followed by a telephone call to the Clerk or the Chairman to confirm that the report has been received.

Should neither the Clerk nor the Chairman be available, the Vice-Chairman of the Council should be informed.

Should the Vice-Chairman not be available all remaining Councillors should be notified.

Reporting Point Responsibilities
Upon receipt of a report the following actions must take place:

1. All incidents must be recorded.
2. The time, date and nature of the incident, together with a description and as much detail as appropriate must be logged on an Incident Response Form
3. Any evidence of the breach must be protected.
4. A documented chain of evidence must be maintained.
5. Relevant authorities, individuals and the media must be liaised with where appropriate.
6. A note of all communications together with their date, time, who has been communicated with, must be kept.
7. The content and nature of all communications must be logged on the Incident Response Form.

Incident Response Plan
Following the correct recording of the incident the following processes must take place.

1. Assessment of the risk to individuals as a result of the breach. The following must be considered:
   a. The categories and approximate number of individuals concerned;

b. The categories and approximate number of personal data records concerned;
c. The likely consequences of the personal data breach, in particular consideration must be made of whether the impact will result in a risk to the rights and freedoms of individuals.
d. Help to assess the risks can be obtained from the Information Commissioner Office (ICO) website;
    i. https://ico.org.uk/for-organisations/report-a-breach/
    ii. https://ico.org.uk/for-organisations/guide-to-the-general-data-proection-regulation-gdpr/personal-data-breaches/

2. If the incident is deemed to be a notifiable incident the following actions must be taken:
    a. Within 72 hours of becoming aware of the incident (even if all details are not yet available), the ICO must be contacted on 0303 123 1113.
    b. The following information must be provided.
        - What has happened
        - When and how the Council found out about the breach
        - The people (how many) that have been or may be affected by the breach
        - What the Council are doing as a result of the breach
        - Who else has been told
    c. For reporting a breach outside normal working hours the ICO Reporting Form should be used.
    https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/
    d. If the incident is deemed to result in a high risk to the rights and freedoms of individuals:
        i. Within 48 hours the affected individuals must be informed by telephone, letter or email about the incident as there may be a need for them to take actions to mitigate risk of damage to them.
        ii. The individuals must be told in clear and plain language
            - The nature of the personal data breach
            - A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, the measures taken to mitigate and possible adverse effects
            - The name and contact details of the Clerk and the Chairman from where more information can be obtained.

3. If the incident is not deemed to be notifiable the following actions must be taken.
    a. Update the Incident Response Form along with the outcome of the risk assessment
    b. Include the steps and evidence used to identify and classify the risk. Include reasons why the incident is not deemed to result in a risk to the rights and freedoms of individuals.

<u>Incident Review</u>

The Clerk and Chairman must ensure that the incident is reviewed at the next appropriate Council meeting under the “Policy and Security” section of the agenda.

a. The Council will consider whether the discussion of the incident warrants exclusion of the press and public from the meeting during that discussion.
b. At the meeting the Council should determine if there are any further actions that need to be assigned or completed as a result of the incident.
c. The Council may decide to refer further actions to a Committee, Working Party or external parties.
d. It should be noted that this final stage of the incident may require a review of this policy document.

This policy will be reviewed annually.