

PRESTON-UNDER-SCAR PARISH COUNCIL

Security Incident Policy

Date for Review: February 2020

What is a breach?

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.

Policy

This policy specifies the actions with respect to breaches of personal data.

Example – 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

Dealing with an incident

Reporting Point

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 of the Council and the Council Chairman
2. The email report should be followed by a telephone call to the Clerk or Council Chairman
3. Should neither the Clerk or Chairman be available, another Parish Councillor should be informed

Reporting Point Responsibilities

All incidents must be recorded. The reporting point shall perform the following actions:

- Note the time, date and nature of the incident together with a description and as much detail as appropriate on an Incident Response Form

- Ensure the protection of any evidence and that a documented chain of evidence is maintained
- Liaise with relevant authorities, individuals and the media where appropriate
- Keep a note of all communications together with their date, time, who has been communicated with, and what the content and nature of communication was on the Incident Response Form

Incident Response Plan

1. Assess the risk to individuals as a result of a 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 consider if the impact results in a risk to the rights and freedom of individuals
 - d. to help assess the risks, refer to the Information Commissioners Office (ICO) website
2. If the incident is deemed to result in a high risk to the rights and freedoms of individuals:
 - a. 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 immediate risk of damage to them
 - b. The individuals must be told in clear and plain language:
 - i. the nature of the personal data breach
 - ii. a description of the likely consequences of the personal data breach
 - 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
 - iv. the name and contact details of the Clerk and Chairman from where more information can be obtained
3. If the incident is **not deemed to be notifiable**:
 - 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
4. **Incident Review:**

The Council Clerk and Chairman will ensure that the incident is reviewed at the next appropriate Council meeting.

- a. The Council will consider whether discussion on the incident warrants exclusion of the press and public from the meeting during that discussion

- b. At that 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. It should be noted that this final stage of the incident may require a review of this policy document

Policy Review

This policy will be reviewed annually or at any other time the Council requires.

February 2019

PRESTON-UNDER-SCAR PARISH COUNCIL

Security Incident Policy

Incident Response Form

Please complete the below and submit to the Parish Council Clerk or Chairman

Date of Incident	Place of incident
Name of person reporting incident	Contact details (Phone / email)
Description of incident and details of information lost	
Reported to	On
Incident Notifiable: YES / NO	If No, please give reasons:
Risk Assessment details / outcome	
Follow up action taken / required (inc date of PC meeting incident reviewed in)	