Felliscliffe Parish Council Security Incident Policy

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 reporting points: The clerk of the council and the council chairman:

email: clerk@felliscliffepc.org.uk

email: cotesyke@hotmail.co.uk

2. The email report should be followed by a telephone call to the clerk or council chairman.

3. Should neither the clerk nor the chair be available the vice-chair of the council 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 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, and;

b. the categories and approximate number of personal data records concerned, and;

c. the likely consequences of the personal data breach, in particular consider if the impact results in a risk to the rights and freedoms of individuals.

d. To help assess the risks refer to 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-protection-regulation-gdpr/personal-data-breaches/

2. If the incident is deemed to be a **notifiable incident** the following actions must be taken:

- Within 72 hours of becoming aware of the incident (even if not aware of all the details yet):

b. Call ICO: 0303 123 1113 – and provide the following information:

- 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; and
- who else has been told.

c. For reporting a breach outside normal working hours use the ICO Reporting Form: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

3. If the incident is deemed to result in a high risk to the right 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 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;

4. 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.

5. Incident Review:

a. The Council will consider whether discussion of 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. The council may decide to refer further actions and to a committee, working group or external parties.

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

The council clerk and chairman will ensure that the incident is reviewed at the next appropriate Council meeting under the Policy and Security section of the agenda.

Policy Review:

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

Adopted:
27th November 2018

APPENDIX 1
Letter template to notify that personal data has been breached

I write to you to bring to your attention a breach of the Data Protection Act that unfortunately involves your personal data. As you would imagine we have taken this matter very seriously and are investigating the matter / have concluded our investigation into it. The facts in this matter are (give brief explanation of what happened e.g. group email sent rather than a response to a single parishioner)

I am unable for reasons of confidentiality to go into details of my investigation, however I am able to tell you that you (state what remedial action(s) have been carried out / what has been to prevent a reoccurrence, without breaching confidentiality)

If you have any questions or concerns regarding this letter, please get in touch with me. I would again like to apologise for the incident of which you were no doubt unaware.

Yours sincerely,

APPENDIX 2

Letter template in response to notification by service user

Thank you for your letter / telephone call of (date) bringing the incident whereby (state what has happened) to our attention.

We are obliged to you for acting in such a responsible way in contacting us. As you would imagine we have taken this matter very seriously and I have concluded our investigation into it.

The facts in this matter are (give brief explanation of what happened eg group email sent rather than a response to a single parishioner).

I am unable for reasons of confidentiality to go into details of my investigation, however I am able to tell you that you (state what remedial action(s) have been carried out / what has been to prevent a reoccurrence, without breaching confidentiality).

I hope this letter has allayed your fears as to the integrity of your own information and documents and can I again thank you for bringing this case to our attention enabling us to take appropriate action.

Yours sincerely,