Darley and Menwith Parish Council ("The Council") - Security Incident Policy

In order to help protect against personal data breaches, it is recommended that correspondence to anyone outside of the Council should ordinarily be sent by the Clerk and that the Clerk should usually manage the personal data held and used by the Council.

1. This policy

This policy specifies the actions to be taken by the Council with respect to breaches of personal data. Personal data can be taken to mean any writing, image or recording that identifies a person.

A glossary is provided as an appendix to this document to help understand some of the key terms used.

2. 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.

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

Further information can be found here:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

3. Dealing with an incident

A. Reporting

On discovery of an incident either as a result of automatic notification, accidental discovery, manual record checking or any other means, all personnel shall;

a. report the incident to the reporting points: the Clerk (clerk@darleyparishcouncil.org.uk) and the Chairman (chairman@darleyparishcouncil.org.uk).

b. The email report should be followed by a telephone call to the Clerk or Chairman.

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

d. Should the Vice-Chairman not be available all Councillors should be informed by email.

B. Recording

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;
- 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; and
- 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.

C. 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:

https://ico.org.uk/for-organisations/report-a-breach/

https://ico.org.uk/for-organisations/guide-to-data-protection/

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 not aware of all the details yet) 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.

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** this should be noted along with the outcome of the risk assessment. 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:

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.

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 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.

Appendix - Glossary of terms

"Personal data" means information about a particular living individual. This might be anyone, including a customer, client, employee, partner, member, supporter, business contact, public official or member of the public. It doesn't need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data.

"**Notifiable incident"** means a breach that is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals. For example:

- result in discrimination;
- damage to reputation;
- financial loss; or
- loss of confidentiality or any other significant economic or social disadvantage.

In more serious cases, for example those involving victims and witnesses, a data breach may cause more significant detrimental effects on individuals.

This must be assessed on a case by case basis and any decision made may need to be justified to the Information Commissioner.

"**High risk**" means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority. This is a matter of fact in each circumstance and depends on the potential impact of the specific personal data breach.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, those concerned must be notified directly without undue delay.

The duty to notify an individual about a breach does not apply if:

- appropriate technical and organisational measures have been applied to the personal data affected by the breach;
- subsequent measures have been implemented which will ensure that any high risk to the rights and freedoms to individuals is no longer likely to materialize; or
- it would involve disproportionate effort.

Where a communication of a breach would involve disproportionate effort, the information must be made available to individuals in another, equally effective way, such as a public communication.