Security Incident Policy

All data controllers have a responsibility under the Data Protection Act 2018 (DPA) to ensure appropriate and proportionate security of the personal data they hold.

The DPA states that: 'appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'

Planning for a breach is therefore essential; every council should have in place a breach response plan, and should designate, in advance, a breach response team (committee) or officer with to deal with the crisis.

Understanding the issues that arise in a breach situation, and practising managing a breach, are essential to effective breach response. Failure to plan and practise increases the regulatory, litigation and reputation risk to the entire council.

READ:

https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf

What your Security Incident Policy should include:

Dealing with a breach:

- Identify, within the council/parish meeting, the designated person, who is to be notified if there is a breach If this person is away on holiday or otherwise absent – what is the backup plan

- Identify, within the council/parish meeting, the dedicated person or committee responsible for managing (and determining whether a personal data breach has occurred)
- and investigating the breach (this may be the same person as above)
  If this person is away on holiday or otherwise absent – what is the backup plan.

NOTE: Ensure any such person(s)/committee have the decision-making authority to deal with these matters.

What is a breach?

Identifying whether a personal data breach has occurred:

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

Reporting a Breach to ICO

Should the breach be reported to the ICO?

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

A breach response plan:

- Assess the risk to individuals as a result of a breach.
- Notify the ICO of a breach within 72 hours of becoming aware of it (even if not aware of all the details yet)
- Ensure the council/parish meeting is aware of all information it must give the ICO about a breach:

THINK!

Can you provide a description of the nature of the personal data breach including, where possible:

- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Call ICO: 0303 123 1113 – you will need to provide the following information:

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

Notifying those affected by the breach:

Have a process in place to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms – affected individuals must be informed without undue delay.

If **a breach is likely to result in a high risk to the rights and freedoms of individuals,** the GDPR says **you must** inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A '**high risk'** means the threshold for informing individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again, the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

Information which must be provided to individuals (data subjects) when telling them about a breach:

- Describe, in clear and plain language, the nature of the personal data breach and, at least:
- The name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- 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.

Further action:

All breaches must be documented, even if they don't all need to be reported -

The facts relating to the breach must be documented, its effects and the remedial action taken. This is part of the council's/parish meeting's overall obligation to comply with the accountability principle and allows The ICO to verify the organisation's (town, parish council and parish meeting) compliance with its notification duties under the GDPR.

Contact your insurance provider – ensure they are made aware of the breach and the potential impact on the council/parish meeting.

Consider a proactive/reactive statement to the Media (press and social media)

Review the technical and organisational measures for the security of personal data within the town, parish council/parish meeting – and implement changes required to minimise the risk of such a breach reoccurring.

NOTE: Once your incident (breach) response policy is in place, practice managing a breach, run through the process detailed – see if it works, amend accordingly!