Security Incidents Policy

What is a 'Security Incident?'

A Security Incident occurs when the Council's assets (including physical assets) or information are subject to the following (whether actual or attempted, or accidentally or maliciously):

- Loss, theft, destruction, or compromise; or
- In the case of information only, disclosed to unauthorised persons (e.g. outside the Council by email).

Why are we concerned about incidents of this nature?

Because the Council is responsible for the management of substantial physical assets and resources on behalf of the public, including sensitive information, some of which is commercial, and also information about residents, council tax payers, elected members, and fellow employees.

In addition, the Council has a statutory responsibility to look after personal data and report certain types of incident (including those affecting ICT systems) to relevant statutory authorities.

Special rules regarding personal-data security incidents

The Council has a legal responsibility to deal with incidents involving individuals' personal data which may result in physical, material or non-material damage, or loss of control over their information. These include limitation of individual rights, discrimination, identity theft, fraud, financial loss, damage to their reputation, or loss of confidentiality. Cases where there is likely to be a risk to individuals for these reasons have to be reported to the Information Commissioner's Office (ICO).

Additionally, where the incident is likely to result in a high risk to the rights and freedoms of the individuals, the Council has to tell those persons so that they can take action so as to protect themselves.

The Council is responsible for all decisions on whether to report cases to the ICO.

Reporting an incident

The Clerk to the Council will complete the Security Incident Report Form (attached). This is used to alert all concerned of the incident and to commence remedial action.

When to report an incident

Immediately it is discovered, or immediately we are informed of an incident by one of our data processors/contractors/service providers, or other third party.