



Breach of Security Policy

Adopted by the Council on the 26th June 2018, reviewed annually in June

ICO - Report a Data Breach under the GDPR or the Data Protection Act 2018

- From 25 May 2018, if councillors experience a personal data breach, they will need to consider whether this poses a risk to people. Council need to consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. When council has made this assessment, if it's likely there will be a risk then the Clerk must notify the ICO; if it's unlikely there will be a risk then council don't have to report it. Every breach does not have to be reported to the ICO.
- 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.
- For more information about what a personal data breach is and when you need to report it to the ICO, please see the personal data breach pages of their Guide to the GDPR.

How do council report a breach?

- The ICO personal data breach helpline staff can offer advice about what to do when a personal data breach has occurred, including how to contain it and how to stop it happening again. The ICO can also offer advice about whether the data subjects involved need to be made aware of the breach.
- The Clerk can report a breach, by calling the ICO helpline on 0303 123 113. The hours of business are - Monday to Friday between 9am and 5pm (excluding bank holidays). A breach can also be reported online on the ICO website, if council believe it is necessary, outside of these hours.

What information will council need to provide?

The ICO helpline will ask:

- what has happened;
- when and how council found out about the breach;
- the people that have been or may be affected by the breach;
- what council are doing as a result of the breach; and
- who the ICO should contact if they need more information and who else have council told.

The ICO will send the Clerk a copy of the information given to them.

What the ICO do with the information provided;

- When reporting a breach, as much accurate detail as possible should be given. The ICO will use the information provided to decide what should happen next. The ICO may use it to take regulatory action, or to identify data security incident trends. Where appropriate, they may share it with law and cybercrime agencies or other regulators. This may include the National Cyber Security Centre, the National Crime Agency or the National Fraud Intelligence Bureau. The ICO may also share information with other regulators, such as the Financial Conduct Authority. Where an incident is relevant to another country, the ICO may also share the information with appropriate regulatory representatives in that country. More information can be found on the ICO website.
- For more about how the ICO use the information provided, look on their website to view their privacy notice.

This policy will be reviewed annually.