Data Breach Procedure

The General Data Protection Regulation (GDPR) makes it compulsory for us to report a personal data breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it in certain circumstances.

The decision as to what actions to take if we become aware of an actual or suspected data breach, including if we need to report the breach, will be taken by a temporary team of three set up for the purpose taken from the Chairman, Vice Chairman, the committee chairmen or the Clerk. We can seek advice from the ICO if we are unsure what action to take or if we need to report.

What is a personal data breach?

We can only use data for the purpose for which it is collected as identified in our data audit and detailed in our privacy notice. Just because we have access to the data does not mean we can use it or share it.

Our staff and councillors need to be able to recognise a personal data breach which can include:
• access by an unauthorised third party
• deliberate or accidental action or inaction
• sending personal data to an incorrect recipient, this includes inappropriate sharing of email addresses or other contact details
• computing devices containing personal data being lost or stolen or accessed by unauthorised persons
• alteration of personal data without permission.

A personal data breach is a security incident that has affected the confidentiality, integrity or availability of personal data.

Procedure
1. If a data breach is suspected by any member of staff or by any councillor then the designated councillors should be notified so that they can assess the impact of the breach and take a decision on the severity and any actions that need to be taken.

2. We do not need to report every breach to the ICO, we need to investigate and make an assessment.

3. In making an assessment we need to consider the likelihood and severity of the risk to people's rights and freedoms or if it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage, following the breach. If it is likely that there will be a risk then we must notify the ICO with in 72 hours of the breach.

4. If it is also likely that there is a high risk to individuals' rights and freedoms then we must notify the individuals.

5. To report a data breach to the ICO we can contact them by phone or by using their online form. We need to give the ICO a description of the likely consequences of the personal data breach, a description of the measures taken, or proposed to be taken, to deal with the personal data breach and also any measures taken to mitigate any possible adverse effects.

6. We will keep a record of all data breaches including those that are not reported to the ICO or to individuals. The record will include what happened, the effects of the breach, remedial actions taken and a record of our decision-making process.

7. We need to consider any public relations impact and make sure that this is managed.

8. We need to investigate if any training or changes to systems is needed if we suffer a data breach.