

GDPR Data Breach Procedure

The following is the procedure that must be followed relating to a potential breach under GDPR legislation.

- Notify the Data Protection Officer of the suspected data breach
- The Data Protection Officer will instruct a team to investigate the potential breach to establish if it is real
- The impact to individuals and organisations will be assessed
- Notify the Information Commissioners Office (ICO) within 72 hours with details of:
 - The nature of the personal data breach
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the Data Protection Officer
 - 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, where appropriate, of the measures taken to mitigate any possible adverse effects

This is only necessary if the breach could result in:

- Discrimination
- Damage to reputation
- Financial loss
- Loss of confidentiality
- Economic disadvantage
- Social disadvantage
- Notify any individuals concerned if there may be a risk to the rights and freedoms of those individuals
- Resolve breach