**Data Protection**

**Responding to a Data Protection Breach**

GDPR requires that **XXXXXXXXXX** must assess and log all personal data breaches and report serious breaches to the Information Commissioner’s Office (ICO) within 72 hours of being discovered.

Failure to notify the ICO of a personal data breach can lead to fines of €10m.

Data security breaches can happen for several reasons such as:

* Loss or theft of data or equipment on which data is stored
* Inappropriate access controls allowing unauthorised use
* Equipment failure
* Human error
* Unforeseen circumstances such as a fire or flood
* Hacking attack
* ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it

The **XXXXXXXXXX’s** Data Protection Lead (DPL) is responsible for deciding whether a breach needs to be reported to the ICO. In making this decision, the following factors should be taken into account:

* The potential harm to individuals which could arise from the breach
* The volume of personal data lost, released or corrupted
* The sensitivity of the data lost, released or corrupted

If you become aware of a loss or theft of personal data or release or corruption of personal data, please notify the DPL immediately: email *[insert your Data Protection Lead’s email address here]* or phone: *[insert your Data Protection Lead’s phone number here]*

* **XXXXXXXXXX Replace this with your organisation’s name**
* **Tailor the wording to your own organisation’s structure**
* **Remove this text box before saving a final version of the document**