**Personal Data Breach Guide**

**Introduction**

This guide has been produced to raise awareness of what a data breach is, and what steps staff should take if a reach is suspected.

**Flowchart**

**What is a personal data breach?**

|  |
| --- |
| A personal data breach is defined in GDPR Article 4(12) as  *‘A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed’*  There are three types of breaches:   1. Confidentiality breach – unauthorised or accidental disclosure of, or access to personal data 2. Integrity breach – unauthorised or accidental alteration of personal data 3. Availability breach – accidental or unauthorised loss of access to, or destruction of, personal data |

**Common data breaches**

Some breaches are more serious than others, but all should be registered on the data breach register. Some common example of data breaches are

* cyber incidents
* compromised or stolen credentials
* theft of paperwork or data storage devices
* lost phones or laptops
* employee misconduct
* data sent to the wrong recipient.
* unintentionally released or published information
* accidentally clicking on a phishing email
* Aalteration of **personal data** without permission

**What to do?**

As soon as a member of staff thinks there ***may have been*** a breach, steps should be taken to stop any further damage. All suspected breaches should be reported to the line manager and also to the Data Protection Officer (Head of Business Services). A way forward will then be agreed. The DPO will provide guidance, will decide whether or not to inform the ICO and or the data subject and will update the breach register. ‘Near misses’ will also be recorded on the breach register, as they are an important way for us to monitor our data security, and provide valuable information to help us improve.

**Reporting to the ICO**

Personal data breaches must be reported to the ICO unless they are unlikely to result in risk to individual rights and freedoms (Article 33). The report must be made to the ICO within 72 hours of the time we are aware *with a reasonable degree of certainty* that there has been a breach and there is risk (we can do some initial investigating to reach this degree of certainty, before the clock starts running).

|  |
| --- |
| **Informing the data subject**  The data subject must be informed without delay if there is a high risk to their rights and freedoms (Article 34). If we do this, we must use clear and plain language, and include all the details we have sent to the ICO.  Even if there is a high risk, there are three possible conditions when we are not required to inform the data subject (Article 34 (3)):   1. Appropriate technical and organisational measures were taken to protect personal data (eg state of the art encryption) 2. Immediately following the breach we took steps to ensure the high risk was no longer likely to materialise. 3. It would involve disproportionate effort to contact the individual. |

|  |
| --- |
| **Assessing risk to individual rights and freedoms**  Damage to individuals can be physical, material or non-material (eg risk of dissemination, identity theft or fraud, financial loss, or damaged reputation). We should use objective criteria to make the assessment, including   * The type of breach * Nature, sensitivity and volume of personal data * Ease of identifying individuals * Severity of consequences * Any special characteristics placing them at greater risk of danger * Number of affected individuals   Note – if the breach is of special category data, damage should be considered as likely to occur.  Andrea Gabbitas  Head of Business Services  September 2019 |