Understanding data breaches (GUIDANCE FOR ALL STAFF)

What’s new under the new Data Protection Act 2018 and GDPR?

- Under the old Data Protection Act 1998 the University had no obligation to report breaches of personal data to the Information Commissioner’s Office (ICO).
- The new Data Protection Act 2018 and the General Data Protection Regulation (GDPR) a new obligations to report breaches to the ICO within 72 hours has been introduced.
  - The University must notify the ICO if a breach would result in a risk to the rights and freedoms of individuals.
  - The University must also notify the individuals themselves if the breach would result in a high risk to the rights and freedoms of those individuals.

What is a breach?

- GDPR defines a breach 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.”
- People often associate breaches with things like lost laptops or stolen files. However breaches can come in many forms, and sometimes a breach can be as simple as retaining information for too long.
- Breaches can be divided into three broad categories, breaches of confidentiality, integrity and availability.

Confidentiality Breach
An unauthorised or accidental disclosure of, or access to, personal data. Examples include:
- An unencrypted laptop with research data is stolen from an academic’s house.
- Mitigating circumstances details of a student are accidentally sent to the email address of a different student.

Integrity Breach
An unauthorised or accidental alteration of personal data. Examples include:
- A hacker gains access to university systems and changes the grades of all students on a particular course.
- Someone only sorts three out of five columns in a spreadsheet full of research data meaning the information is inaccurate.

Availability Breach
An accidental or unauthorised loss of access to, or destruction of, data. Examples include:
- Boxes of student welfare records (where no electronic version exists) are destroyed by a flood.
- The only copy of research data on thousands of NHS patients is stored on an encrypted hard drive, but the encryption key has been lost.
### Common causes of breaches:

#### Breaches reported to the ICO from the Education Sector

<table>
<thead>
<tr>
<th>Underlying cause of breach</th>
<th>Example</th>
<th>How to avoid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Error</td>
<td>Incorrectly addresses emails, lost paperwork etc.</td>
<td>Training and awareness, care taken when addressing emails and handling information</td>
</tr>
<tr>
<td>Technology</td>
<td>Insecure IT system or a lack of recent virus definitions</td>
<td>Regular patching and careful procurement of IT systems</td>
</tr>
<tr>
<td>Process failures</td>
<td>Lack of safeguards in a process</td>
<td>Develop and communicate robust secure processes to avoid risk</td>
</tr>
<tr>
<td>Malicious behaviour</td>
<td>External cyber attacks</td>
<td>Regular virus definition updates, care when clicking on links/attachments from strangers</td>
</tr>
</tbody>
</table>

#### What can you do?

- Be clear about what a data breach is – make sure you know how to identify when one has happened.
- When a breach has happened immediately report it as a Data Incident on 0116 252 5800
- Ensure that lessons are learned once a breach has occurred to ensure they do not happen again.

#### Further information:

- If you need further information or have questions about data breaches please email the [gdpr@le.ac.uk](mailto:gdpr@le.ac.uk)
- Further guidance the Data Protection Act 2018 and the General Data Protection Regulations is available at: [https://www.le.ac.uk/gdpr](https://www.le.ac.uk/gdpr)