Reporting a Data Breach

Where do I report a data breach?

If you think there has been a data breach, immediately report this to the **DPO (Data Protection Officer), Inderpal Virdee** on 0121 446 4545 Ext: 5478 or 07814 539843 or alternatively email dpo@bmet.ac.uk

You must forward all relevant information related to the breach. Please complete the form online Notification of Data Breach or download a copy of the Notification of Data Breach (Word Doc) and send it to dpo@bmet.ac.uk

If a personal data breach occurs out of hours, then please contact the Duty Director on Tel: 0121 503 8578 ext. 8578. Out of office hours means any time after 5pm Monday – Thursday, Friday any time after 4pm or anytime Saturday or Sunday.

New data breach notification requirements

The DPO, **Inderpal Virdee**, is responsible for ensuring that all relevant data protection breaches are reported to the ICO without delay and no later than 72 hours after having become aware of it, unless the data was anonymised or encrypted.

The DPO will make an assessment of the breach and decide if this should be reported to the ICO in accordance with the reporting methods set by the ICO.

In her absence the following staff should be contacted:

Rich Williams, Ext: 5288, **07747 791162**
Or
Liam Nevin, Ext: 8508, **07834 512630**

It is worth noting that a failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

What is a Data Breach?

A data breach is a security incident in which personal or other confidential information data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

Data means information in any format, e.g., papers, records, emails, faxes etc.

The definition of personal data can be complex and, in the event of a breach, it is safest to assume any information about a living individual is personal data and may include;

- Factual information about an individual such as name, student identification number, date of birth, address, bank account details.

- Sensitive information such as information about mental and physical health, sexual life, criminal records and activities, ethnicity and religion.
- Opinions expressed about an individual for example in staff or student appraisals or email exchanges.

Examples of personal data breaches include:

- leaving paper records on a train;
- email personal data to the wrong person;
- deleting personal data when it is still needed;
- losing a memory stick containing personal data;
- loss or theft of mobile devices containing data about people (e.g., laptops, PDAs, mobile phones, etc.) or loss of hard copy data within briefcases, folders;
- sharing information about people with unauthorised third parties, either accidentally or willfully; and
- sending emails or letters in error to the wrong person(s) or wrong address(es).

Why should breaches be reported?

- The longer an incident goes unreported, the longer a vulnerability may remain unaddressed allowing the incident to escalate or for further incidents to occur.
- Without timely visibility of the incident through reporting we may not be able to fulfil legal obligations. The General Data Protection Regulations (GDPR) places a duty on organisations to report certain types of personal data breach to the Information Commissioner's Office. Knowing that a breach has occurred and delaying reporting reduces the time available for the investigation team to understand and assist with a response and still meet legal compliance. Where the breach does not affect personal data, time is still critical and may have contractual implications.
- Understanding the cause of breaches allows us to develop and implement systems and processes that are more robust and so prevent future breaches.

Who should report?

- All employees, contractors and temporary workers.

What happens after the report is made?

- The Data Protection Officer will make an initial assessment to determine the next steps.
- The severity of the incident will inform and direct the appropriate level of leadership involvement.
- An investigation may be conducted using a variety of techniques and tools, including interviews and site visits.
- The outputs of the investigation may include corrective and preventive actions, formal reporting or other communications.