Reporting a Data Breach and "Near Misses"

Where do I report a data breach and "near misses"?

If you think there has been a data breach, immediately report this to the **DPO (Data Protection Officer), Michael Lewis** on 07526 178790 or alternatively email dpo@bmet.ac.uk

Where a data storage device such as a PC, laptop, tablet, USB stick, or smart phone has been lost or stolen regardless of the data it contains - immediately contact both the DPO at dpo@bmet.ac.uk and the IT Service desk team at itservicedesk@bmet.ac.uk

A data breach could be as simple as you putting a letter in the wrong envelope and therefore even the most minor data breaches must be reported.

False alarms or even breaches that do not cause any harm to individuals or to the College should nevertheless be reported as it will enable us to learn lessons in how we respond and the remedial action we put in place.

We have a legal obligation to keep a register of all data breaches, no matter how big or small and no matter whether any harm was caused. Please ensure that you do report any breach, even if you are unsure whether or not it is a breach.

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 the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. The College has only 72 hours to report a breach to the Information Commissioner's Office.

New data breach notification requirements

The DPO, 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 during office hours:

Rachel Jones, Ext: 5290, **07807 341243**
Or
Stephen Belling, Ext: 8508, **07526 178783**

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 reportable breaches and "near misses"

While this list is non-exhaustive it does give examples of some of the more common data breaches and 'near misses' that should be reported.

- leaving paper records on a train;
- 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;
- sending emails or letters in error to the wrong person(s) or wrong address(es); and
- any 'near miss' incident that had the potential to cause a data breach even though it might not have done so.

Mitigation of personal data breaches - Steps required to contain and mitigate the breach will be identified, documented and undertaken. These may include:

- immediately recalling an email that has been sent to the wrong address;
- contacting the recipient of an email that has been sent in error and asking them to delete the email from their inbox and deleted items and confirm they have done so;
- immediately retrieving paper documents from any unintended recipients;
- changing the password for the affected application, device, system or room;
- immediately disabling any lost or stolen electronic devices;
- notifying colleagues of any immediate steps that they should take;
- remotely locating, disabling and/or deleting data stored on a mobile device;
- restoring a database or system from a back-up;
- disabling network or system access; and
- notifying staff and/or Processors to do or refrain from doing something.

All actions need to be appropriate, proportionate and accountable.

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.