Data Breach Policy

2021-2023

Approved by: Academic/Quality Assurance Board

Date of approval: 30/05/2021

Effective date: 30/05/2021

Next review date: 30/05/2023

VERSION: 002

Data Breach Policy

In the event of a data breach – which we define as any circumstance when data has or might have been removed or copied and/or taken from outside of our control – the following will occur

- A breach log ("Breach Log")will be set up to record breaches
- The first person to identify or suspect the breach will immediately inform the DPO (dpo@mrcollege.ac.uk)
- The DPO will or will arrange to investigate and will assess as soon as possible whether there is a breach and if so what has been removed or otherwise breached and whether it could be considered as a breach posing a risk of harm to the Data Subject
- Any breach involving losses of multiple sets of data will be considered as likely to pose a risk of harm
- If there is no risk of harm to the Data Subject the DPO will:

  - Note the breach in the Breach Log

  - Take steps to ensure that it cannot happen again including where necessary providing additional training
- If there is a risk of harm the DPO will:

  - Will ensure to have robust breach detection, investigation and internal reporting procedures in place.

  - Report to ICO and those affecting individuals within 72 hours using the template letter

  - Advise the relevant data subjects using the template letter

  - Note the breach in the Breach Log

  - Takes steps as above to ensure it cannot happen again

  - Take such other steps as are reasonably required

  - Comply with any requirements of the ICO