**Data Incident Reporting of a Personal Data Breach:**

What is a personal data breach?

* A personal data breach is when “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, confidential data transmitted, stored or otherwise processed.” While all personal data breaches will be security incidents, not all security incidents will be personal data breach.
* When a personal data breach occurs, we must consider its significance and whether this poses a risk to people. Therefore, an assessment must be made quickly and if there is likely to be a risk we must notify the Information Commissioners Office (ICO) within 72hrs of identifying the breach; if it is unlikely then we do not have to report. Failure to report a significant breach means we could be heavily fined by the ICO. Completion of the University Data Incident Reporting form at the earliest opportunity will enable this assessment to be made.

This guidance relates to any actual, suspected, threatened or potential personal data breach, including near misses. Find examples of personal data breaches below:

* Opening or clicking a link within a malicious email which contains malware or viruses
* A ransomware attack whereby access to systems or records containing personal data is disabled or encrypted
* A cybersecurity attack whereby personal data is accessed, altered, deleted and/or disclosed by the attacker
* Human error, for example an email attachment containing personal data being sent to the incorrect recipient or records being deleted accidentally
* Sharing of passwords or other credentials with third parties
* Controlled documents being left unattended to be copied, read or photographed by an unauthorised person
* ‘Blagging’ whereby an individual obtains personal data by deception
* Unlawful interception of email or telephone communications or online form submissions
* Loss or theft of a physical file or electronic device containing personal data
* Loss of a decryption key relating to securely encrypted personal data
* A Denial of Service (DoS) attack preventing access to personal data for a period of time
* Damage caused by unforeseen circumstances such as fire or flood