DATA BREACH PROCEDURE

1 What constitutes a breach:

1.1 The 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"* by the University or one of its subsidiary companies.

1.2 All breaches or suspected breaches, regardless of severity, must be reported immediately to the Data Protection Officer ("DPO") once the staff member becomes aware of it using the procedure detailed below in paragraph 2 below.

1.3 The following are examples of breaches that must be reported to the DPO. **Please note:** This list is not exhaustive and if in doubt staff should consult the DPO:

- Loss of personal information such as email addresses, names, bank details, medical records etc.
- Personal information of data subject(s) sent to the wrong person.
- Loss of a portable device containing personal information such as laptop, mobile phone, USB memory sticks etc (regardless of whether encrypted or password protected).
- Accidental destruction of a database containing personal information.
- A cyber attack leading to the theft of data.
- Papers containing personal information left on a desk or open cupboard that may have lead to unauthorized access.
- A member of staff "ccing" instead of "bccing" a group of students in an email.

2 Reporting Procedure

2.1 During Office Hours

During office hours, staff should contact the DPO via extension 5264 (01707 285264) or by email dataprotection@herts.ac.uk, marked as urgent, with the subject line "DATA PROTECTION BREACH"

2.2 Out of office hours

Out of office hours, staff should telephone 01707 285900 (DPO out-of-hours mobile).

2.3 When reporting the breach the member of staff should, where possible, provide the DPO with the following information:

- Data Subjects affected (categories and number of individuals affected).
- Information categories concerned eg names, email address, bank details etc.
- How the breach occurred.
- When the breach occurred.
- When staff member became aware of the breach.

3 DPO Duties

The DPO will:

3.1 decide, in consultation with senior management, if the breach is severe enough to require reporting to the ICO and, if applicable, the data subjects affected;

3.2 inform the ICO using the ICO's reporting mechanism available at https://ico.org.uk/for-organisations/report-a-breach/ within 72 hours of the member of staff becoming aware of the breach;

3.3 inform data subjects using the standard letter template available from the Data Protection Officer within 72 hours of the member of staff becoming aware of the breach; and

3.4 keep a register of all breaches and provide recommendations to staff regarding any remedial action to be taken.

Mrs S C Grant
Secretary and Registrar
Signed: **25 May 2018**