St Stephen's House, Oxford - Personal data breach – required procedure

Personnel Process

1. If a possible breach has been made, immediate notification should be made to the Data Protection Officer, to the Bursar, or to the Principal. A double check of the data procedures used should then be carried out.

2. No more of the procedures that led to the possible data breach should be carried out, until the investigation has been completed.

Management and Personnel Process

1. The person who has had the possible breach must let their immediate line manager or Head of House know what has happened. This notification should be carried out within 30 minutes of becoming aware of the possible breach.

2. The immediate line manager or Head of House should let the College Data Protection Officer (DPO) know of the possible breach when it first comes to their attention (within 30 minutes). Information provided by the user about the possible breach should be made available to the DPO as soon as possible.

3. The DPO will then look at the current information and start an investigation. The investigation process will need to be drawn up by the DPO, following a procedure agreed by the College – this must include consideration of the need to notify the individual that there has been a breach in relation to their data. If the breach involves University data then the DPO must contact the University Information Compliance Team (ICT) University Data Protection Officer/ Senior Information Compliance Officer. Similarly the DPO should contact the University where the breach may result in reputational/ financial risk (whether or not this relates to University data). The University Information Security Team (IST) should also be contacted when the breach relates to IT Infrastructure.

4. In all other cases the DPO can reserve the right to seek the advice from the central University Information Security Team (IST) and/or Information Compliance Team (ICT) on any matter that is non- trivial.

5. The investigation should be a swift process, taking no more than 2-3 days (72 hours) at maximum as specifically required under GDPR - see https://ico.org.uk/for-organisations/guide-to-the-general- data-protection-regulation-gdpr/personal-data-breaches/. Reporting to, or seeking advice from the University must also be within the 72 time period so that there is no delay should a breach need to be reported to the ICO.

6. Depending on the nature of the breach, it may also be necessary to report the issue to the UK Charity Commission.

Document version 1.1, revised for minor errata and format, August 2018