Personal Data Breach Reporting Procedure

Under the UK General Data Protection Regulation (UK GDPR) the College is required to keep a log of all personal data breaches and in certain circumstances there is an additional requirement to inform the Information Commissioner's Office of such a breach.

This procedure covers any incident where it appears there has been a personal data breach. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Personal data breaches can include:

- access to an IT system by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- receiving personal data in error;
- publication of personal data on the website;
- College-owned computing devices containing personal data being lost or stolen;
- personal computing devices used for work purposes containing personal data being lost or stolen;
- paper records containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

This document describes the procedure for reporting incidents which constitute a suspected personal data breach. It applies to all personal data made available to the university, irrespective of the source of the data or the media upon which it is held, and encompasses all College activities.

Reporting and immediate action

If you suspect a data breach has occurred, report it to your line manager, principal investigator or supervisor immediately. You are required to make an initial assessment of the incident and complete the relevant parts of the Reporting a Data Breach form. The form should be sent to dataprotection@royalholloway.ac.uk without delay and marked as Data Breach.

If you are unsure whether or not a data breach has occurred, report it.

If the IT Service desk receives a report of a data breach, a security risk or the loss of an IT asset which may contain personal data, this should be reported in the manner outlined above. The Head of Information Security should also be informed.

The report of the breach will be considered by the Data Protection Officer or their nominee and they will advise on the next steps to be taken and will determine whether the breach must be reported to the Information Commissioner's Office.

Investigation

Minor Breach

If the breach does not need to be reported, the reason for this will be documented. The Data Protection Officer or their nominee will conduct an internal investigation with the relevant staff

including the reporting member of staff, their line manager and the relevant Data Steward(s) and Data Custodian(s) if not already involved. If there is an aspect of the case relating to technical security or devices supplied by IT Services, the Head of Information Security or their nominee will also be consulted.

Upon the conclusion of the investigation, the Data Protection Officer or their nominee will write a report of the incident including any recommendations and update the data breach log. In certain circumstances, the report will be shared with the College's Executive Team.

Major Breach

If the breach is sufficiently serious to be reported to the Information Commissioner's Office, in that it is likely to result in a risk to the rights and freedoms of individuals, it must be reported no later than 72 hours after someone in the College becomes aware of it.

The Data Protection Officer will co-ordinate a working party to assess the breach, investigate it and decide upon the College's response. This group may include the following individuals as appropriate to the investigation:

- Head of Information Security
- Relevant Data Steward(s)
- Relevant Data Custodian(s)
- Relevant Head of Department or Professional Service
- Director of Marketing and Communications or nominee

Upon the conclusion of the investigation or upon reaching the 72 hour deadline, whichever is sooner, the Data Protection Officer will report the breach to the Information Commissioner's Office in accordance with their requirements. An internal report will also be generated and shared with the College's Executive Team and the Master Data Management and Reporting Group.

If there is a high risk to the rights and freedoms of individuals, they must be informed without undue delay. The Data Protection Officer will liaise with the Director of Marketing and Communications or their nominee to agree a plan of communication with affected data subjects and prepare any external press statements.

Action and follow-up

Following the conclusion of the investigation, remedial actions or improvements may have been identified. This may include an evaluation of relevant procedures to determine whether improvements can be made, identification of additional training requirements and testing of IT systems.

Any agreed actions will be confirmed by the working group established to investigate the breach and will be included, along with a timescale for completion, in the report shared internally.

Approved by Planning and Resources Committee – May 2018
Reviewed date – December 2020
Next review – December 2022