Procedure

Goldsmiths
UNIVERSITY OF LONDON

Data Breach and Information Security Incident Reporting Procedure

Owner: Senior Information Risk Officer
Review date 20 May 2019

1. Introduction

1.1 The College holds and processes large amounts of data and information. It has legal and moral responsibilities for protecting this data and information so that the rights and freedoms of individuals as well as the commercial and educational interests of Goldsmiths and its partners are secured.

1.2 When handling data and information on behalf of the College, due care and attention should be taken not to do anything that may put at risk the integrity or security of data and information.

1.3 In the event of a data breach or any other information security incident, appropriate action is to be taken to actively manage the situation so as to minimise the impact of the same.

2. Purpose

2.1 This document sets out the procedure that is to be followed upon any data breach or information security incident.

2.2 Adherence to this Procedure will ensure the College's response to and management of breaches and incidents is consistent and effective.

3. Scope

3.1 This Procedure is to be followed by all those who hold and/or process the College's data and information, including staff, students and third parties who hold and/or process on Goldsmiths' behalf.

4. Related Policies

4.1 This Procedure is related to the following Goldsmiths policies:

i) Data Protection Policy;

ii) Information Security Policy; and

iii) Protective Marking Policy.

5. Responsibilities

5.1 All those who handle or process Goldsmiths information must be familiar with this Procedure and comply with its terms.

5.2 All those who handle or process Goldsmiths information are responsible for reporting any data protection breach or information security incident in accordance with the terms of this Procedure.

5.3 The Senior Information Risk Owner, the Chief Information Officer, the Data Protection Officer and the Information Security Officer have specific responsibilities under these Procedure. They shall be familiar with this Procedure and comply with its terms.

6. Compliance

6.1 Responding promptly and effectively to data breaches and information security incidents ensures compliance with the College's legal and moral obligations and will minimise the risk to the confidentiality, integrity and availability of Goldsmiths information as well as the rights and freedoms of individuals.

6.2 All whom this Procedure applies to must comply with its terms. Failure by any relevant person to do so may result in disciplinary action being taken against them. Failure to comply with the terms of this Procedure by an organisation to whom it applies, may result in the termination of contractual relations.

6.3 The Data Protection Officer shall monitor compliance with the Procedure and provide report in respect of the same to the Senior Information Risk Owner.

7. Information Security Incident

7.1 An information security incident causes or may cause the loss, damage, non-availability or unauthorised disclosure of College information. The following are examples of incidents:

i) loss of paper records containing personal data or commercially sensitive;

ii) loss of equipment on which personal data or commercially sensitive information is stored (e.g. mobile phone, laptop, iPad or USB stick);

iii) unauthorised or accidental use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems);

iv) disclosure of sensitive or personal information (e.g. email or document sent to an unintended recipient or posted in the public domain);

v) loss, damage or destruction of personal data (e.g. as a result of changes or deletions made by staff of documents stored on College IT systems);

vi) disturbance of IT systems results in data being unavailable;

vii) account of any College IT user is compromised (e.g. login details shared with others or obtained via a phishing email); and

viii) cyber attack diminishes availability of IT services or compromises the security of College systems.

8. Reacting to and reporting a personal data breach or any other information security incident

8.1 Upon discovering any personal data breach or any other information security incident, staff should report this immediately by completing a report form. In the event that it is not possible to complete the form, staff must:

i) contact the Data Protection Officer at dp@gold.ac.uk; and

ii) contact the Information Security Officer at P.Hircock@gold.ac.uk.

8.2 The Data Protection Officer or the Information Security Officer shall maintain a register of incidents as appropriate, which shall include any investigations carried out and actions taken.

8.3 The Senior Information Risk Officer and the Chief Information Officer shall be notified forthwith of any information security incident by the Data Protection Officer and the Information Security Officer.

9. Investigation

9.1 All incidents will be investigated in order to establish the nature of the incident, what data and information has been affected by the incident (including its category) and the consequences of the incident (e.g. loss of IT systems or infringement of rights and freedoms of individuals). Investigation will commence as soon as reasonably practicable.

9.2 Investigation of a personal data breach will support a determination of whether the matter needs to be reported to the Information Commissioner's Office. An investigation of a personal data breach will assess the nature and category of the personal data affected, whose data is affected and the risk to the rights and freedoms of those affected.

10. Notification of personal data breaches

10.1 Where, in the opinion of the Data Protection Officer, it is considered likely that the rights and freedoms of an individual are at risk as a result of a personal data breach, they will notify the Information Commissioner's Office no later than 72 hours following discovery of the breach.

10.2 Where, in the opinion of the Data Protection Officer, it is considered likely that the personal data breach will result in a high risk to the rights and freedoms of an individual, they will notify the affected individual as soon as possible or direct another to do so.

10.3 The Data Protection Officer will maintain a register of all personal data breaches discovered, regardless of whether they have been reported to the Information Commissioner's Officer or the affected individual has been notified.

11. Incident response management

11.1 An early, coordinated and well resourced response to an information security incident can minimise its impact. Upon being notified of an incident, either the Senior Information Risk Owner or the Chief Information Officer may convene a management response team to coordinate and direct the College's response. The team shall include the Data Protection Officer and the Information Security Officer and such other staff as may be appropriate.

12 Incident review

12.1 Following the investigation of an incident, a review will be conducted and recommendations made. This review will be led by the Information Security Officer.