Royal College of Art
Postgraduate Art & Design

Data Breach Management Procedure

1.0 Introduction

1.1 All members of the College including staff, students and others acting on behalf of the RCA are responsible for safeguarding the personal data they process in accordance with the College's Data Protection policy.

1.2 The Data Protection Officer may recommend the instigation of the relevant disciplinary policy for staff, or misconduct procedure for staff or students, where evidence of non-compliance with the Data Protection Policy, of which this Personal Data Breach Management Procedure forms a part.

2.0 Purpose

2.1 The purpose of this procedure is to standardise the College's response to any reported personal data breach incident and ensure all incidents are managed with respect to legal and regulatory requirements and best practice guidelines.

2.2 The implementation of this procedure will ensure that:

- incidents are reported and properly managed in a timely manner;
- incidents are handled by appropriately authorised and skilled staff members;
- incidents are suitably recorded and documented;
- the impact of data breaches is understood and that the required follow up actions are taken.

3.0 Definitions

3.1 Data breach: this is defined in Article 4(12) of the General Data Protection Regulation 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.'

3.2 Data subject: the individual to whom the personal data relates.

3.3 Personal data: any information relating to an identifiable person who can be directly or indirectly identified.

4.0 Royal College of Art Breach Management Process

4.1 All data breaches must be reported as a matter of urgency and should be reported to the Data Protection Officer **data-protection@rca.ac.uk** without unnecessary delay so that the seriousness of the breach can be determined as soon as possible. This includes all types of data that is held by the College, including material that belongs to third parties and is held by the RCA (e.g. research data) and also RCA material which is managed by third parties (including third party data processors under contract to the RCA).

4.2 Once a data breach has been reported, its management has four elements:

- **Containment** and recovery to limit damage as far as possible.
- **Assessment** of risks to help inform decisions about remedial actions and notification.
- **Notification** to the appropriate bodies/individuals that a breach has occurred.
- **Evaluation** of the causes of the incident and the effectiveness of the College's response, identifying lessons to be learned.

4.3 Processors (third party companies providing services on the College's behalf) are legally obliged to notify the College of all data breaches under Article 33(2) of the GDPR. Notification must be without undue delay after the processor becomes aware of the breach.

5.0 Examples of what should be reported

5.1 A key principle to consider:

If in doubt, report it.

5.2 Human error

- Personal data emailed, posted or handed to the wrong recipient
- Excessive/non-essential personal data provided to otherwise valid recipients
- Personal data received in error
- Loss of hard copy material containing personal data
- Loss of any RCA-owned[1]* data storage device, regardless of the data it contains, e.g. laptop, PC, USB drive, tablet, removable hard drive, smart phone or other portable device
- Unauthorised publication of personal data on a website or social media channel

[1] Loss of any privately-owned devices should only be reported if they contain personal data related to College activities

5.3 Theft

- Theft of hard copy material containing personal data
- Theft of any College-owned[2] data storage device, regardless of the data it contains, e.g. laptop, PC, USB drive, tablet, removable hard drive, smartphone or other portable device

5.4 Malicious intent

- Attempts (either failed or successful) to gain unauthorised access to university systems, e.g. hacking
- Virus or other malicious malware attacks (suspected or actual)
- Compromised user accounts, e.g. disclosure of user login details through phishing
- Information obtained by deception ("blagging")
- Deliberate leaking of personal data

5.5 Malfunctions

- Failure of software or hardware leading to personal data loss
- Damage or loss of personal data due to fire, flood, power surge or other physical damage

[2] Theft of any privately-owned devices should only be reported if they contain personal data related to university activities.