LFS Data Breach Policy

1. Introduction

This policy is to explain organisational and technical measures taken by the London Film School ("LFS", "we", "our", "us") to prevent, identify, and if required, manage and report data breaches involving people connected with us, including, but not limited to applicants, students, staff and contractors ("you", "your").

2. Purpose of Data Breach Policy

We hold and process large amounts of data and personal information in line with our privacy policies. The purpose of this policy is to ensure that anyone involved in holding or processing data understands the need for careful handling of such data to prevent unauthorised access or disclosure, loss, unauthorised destruction, or alteration ("data breach", "data breaches").

This includes data breaches caused by human error for which we may be vicariously liable, malicious intent or failure of systems.

Further, the purpose of this policy is also to remind anyone holding or processing data of the potential loss of trust, fines, disciplinary actions and payment of compensation to data subjects affected by a breach.

This policy should be read in conjunction with the LFS Data Classification Policy and the various LFS Privacy Policies.

3. Scope

This policy applies to anyone holding or processing data or personal information as per the LFS privacy policies, including, but not limited to staff and contractors. It also applies to students who handle personal information of other students, staff, contractors or third parties (such as actors, external crew members, etc.).

4. Data Breach Incidents

The following describes what may constitute a data breach:

1) Accidental loss or theft of data or information classified as 'restricted' or 'confidential' as per the LFS Data Classification Policy, including, but not limited to:
    a) Loss of paper records
    b) Loss of laptop or other personal computer that may contain classified data or personal information;
    c) Loss of mobile phone (work or personal) that may contain classified data or personal information;
    d) Loss of tablet or other portable device (work or personal) that may contain classified data or personal information;
    e) Loss of USB stick or other portable storage device (work or personal) that may contain classified data or personal information;
    f) Loss of any magnetic or optical media (work or personal) that may contain classified data or personal information;
2) Unauthorised use, access to or modification of data or information systems, e.g. sharing of user login details (deliberately or accidentally) that enables an unauthorised user to gain access and/or to make unauthorised changes to data or information systems;
3) Accidental unauthorised disclosure of sensitive or confidential information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee);
4) Intentional unauthorised disclosure of sensitive or confidential information;

5) Compromised user account (e.g. accidental disclosure of user login details through phishing)
6) Failed or successful attempts to gain unauthorised access to LFS information or information systems;
7) Equipment failure that leads to unauthorised access, disclosure or sharing of classified data or personal information;
8) Disruption to or denial of IT services;
9) Unauthorised publication of classified data or information on LFS website or other public or semi-public platforms (e.g. Moodle).

5. Reporting Data Breaches

First and foremost, it is the responsibility of the individual who causes or identifies the potential data breach to report the data breach without delay using the online form or by emailing the Data Protection Officer (DPO) at dataprotection@lfs.org.uk.

Individuals reporting a data breach are encouraged to report as many details about the breach as possible to enable us to efficiently and effectively investigate the breach. As a minimum, this should include a description of the data lost, including an estimation of the amount of data that was lost, details of what caused the data loss (if known), persons and systems involved, and whether the cause of the breach was temporary or is ongoing and requires immediate action to be taken.

Where immediate action is to be taken, the breach should not only be reported via the online form or email, but also in person.

6. Investigating Data Breaches

1) Upon receiving a report of a potential data breach, the DPO (or their nominee) will investigate the potential breach using both the information provided by the individual who reported the breach and any additional information available to them. Any investigation will normally commence within one working day of the potential breach being reported.
2) The investigation and any materials associated with the investigation, including notes, logs, CCTV footage, etc. will normally be treated as confidential unless we are obliged under a legal, contractual or regulatory duty. Wider notification must be agreed by the DPO.
3) Materials used as evidence may be kept beyond their normal retention periods.
4) Additional information may be obtained by interviewing the individual who reported the breach as well as any other parties involved or associated with the potential breach and, if appropriate, by reviewing logs from IT or other systems. CCTV footage may also be reviewed, if required.
5) Anyone involved in or associated with the potential breach is required to cooperate with the investigation in full and without delay.
6) The investigation will seek to establish the nature and severity of the data breach, the data subjects affected, and the number of records breached. In establishing severity, the DPO will take both LFS Data Classification Policy and the number of data subjects potentially affected into consideration.
7) The status and findings of the investigation may be reported to third parties where this is required by law or where legal action is being taken or where there are other legal responsibilities. The DPO will also determine whether the Information Commissioner's Office (ICO) is to be informed, normally within 72 hours of the notification of a potential breach.
8) Depending on the severity of the data breach, the DPO may choose to provide the Board of Governors with updates of an ongoing investigation as well as a summary reports upon conclusion of the investigation.
9) The DPO may recommend the instigation of disciplinary action where an investigation concludes that a failure to adhere to this or other relevant policies caused or risked causing a

data breach. Where such action is recommended following the conclusion of the investigation, the findings may be passed on to HR and the relevant line manager.

7. Containment and Recovery

Appropriate steps will be taken wherever possible to recover, render unusable, or remotely delete (if possible) lost or stolen data or personal information. Immediate actions may include changing user passwords, and/or temporarily blocking user accounts until the full nature and severity of the data breach has been established.

8. Notification

The DPO is ultimately responsible for determining whether a data breach is considered reportable and will, if required, contact the relevant authorities.

Where possible and appropriate, data subjects whose personal information has been compromised will be informed of the data breach in a timely fashion regardless of whether the incident is deemed 'reportable' to enable then to take steps to protect themselves. The notice will include a description of the data breach and the steps taken to contain and/or mitigate the risks.

9. Review and Evaluation

After the conclusion of a data breach investigation, the DPO will provide a summary report of the data breach to the Management Team where consideration will be given to the need to review any of LFS's policies or procedures to avoid future breaches.

10. Version Control

Version Number	Changes	Author, Title	Date
0.1	-	Moshe Nitzani, IT Manager	14/05/2018
0.2	Amendments from Acting COO and comments from GDPR working group added	Dan Lawson, Acting COO	23/05/2018
0.3	Review by Philip Ramge, Academic Registrar	Philip Ramge, Academic Registrar	18/06/2018
0.4	Further revisions by Dan Lawson, Acting COO incorporating comments from GDPR working group	Dan Lawson, Acting COO	03/07/2018
1.0	Approved by Management Team	-	10/09/2018