LFS Data Classification Policy

1. Introduction

This policy aims to explain how the London Film School ("LFS", "we", "our", "us") classifies different types of data used in the conduct of our business, particularly personal information and data held about different kinds of data subjects ("you", "your").

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

2. Purpose of the Data Classification Policy

The purpose of this policy is to offer guidance to members of staff or contractors involved in the collection, storage and processing of personal information and data. Further, it informs the technical and organisational measures implemented by us to protect against data breaches, as described more fully in the LFS Data Breach Policy.

Finally, it provides anyone who collects, stores or processes personal information or whose personal information is being collected, stored or processed by us with information about how their data is classified and treated to avoid breaches.

3. Data Classification

The table below provides information about the different types of classification, including examples, risks attached to certain types of data, mandatory and optional methods of protection available and provides guidance to members of staff and contractors on collecting, storing and processing personal information and data using our systems and processes.

3.1. Confidential

Impact: High

If breached, personal information or data classified as 'confidential' could seriously affect the privacy of affected data subjects, cause serious damage to our reputation, or have substantial financial effects on us, the data subject or a third party.

Data classified as 'confidential' is only available to designated or relevant members of staff or contractors.

Data classified as 'confidential' would not normally be available to third parties unless the third party has a legitimate interest or there is a contractual, statutory, regulatory or otherwise legal obligation.

3.2. Restricted

Impact: Medium

If breached, personal information or data classified as 'restricted' could have an intermediate impact on the privacy of data subject, cause damage to our reputation, or have financial effects on us, the data subject or a third party.

Data classified as 'restricted' is available to members of staff and contractors on a need-to-know-basis and to students were the information relates to the student directly.

Data classified as 'restricted' would not normally be available to third parties unless the third party has a legitimate interest or there is a contractual, statutory, regulatory or otherwise legal obligation.

3.3. Internal

Impact: Low

If a breach were to occur in this category, it may have minor impact on the privacy of data subjects, cause some minor reputational damage, or have minor financial effects on us.

Data classified as ‘internal’ is available to all members of staff and contractors but would not normally be available to third parties unless the third party has a legitimate interest or there is a contractual, statutory, regulatory or otherwise legal obligation.

3.4. Public

Impact: None

4. Data Classification Table

	Public	Internal	Restricted	Confidential
Examples	Any information which is in the public domain; press releases; course information; names, photos and biographies of members of staff, contractors and Governors; some policies.	Professional contact information of staff, contractors and Governors, internal phone numbers; some policies, procedures and guidelines.	Personally identifiable information, including names of those not included in the 'Internal' category, phone numbers, addresses, date of birth; details of applications submitted by prospective students or job candidates.	Bank details; financial data; students' academic records, including coursework, assessments and results; medical records of students and staff; notes, minutes and decisions of disciplinary, complaint or other investigations or hearings; passwords; contracts; equal opportunities monitoring data (if not anonymised); market sensitive information.
Protection	None	Access is limited to members of staff and contractors; digital information is only to be stored on password-protected computers using personal LFS login details and must only be stored on LFS-approved systems with enforced access control mechanisms; paper files must never be left unattended in public rooms or spaces.	Access is limited to members of staff and contractors on a need-to-know basis; digital information is only to be stored on password-protected computers using personal LFS login details and must only be stored on LFS-approved systems with enforced access control mechanisms; paper files must not be left unattended for prolonged periods of time in private LFS offices; paper files must never be left unattended in public rooms or spaces.	Access is limited to designated or relevant members of staff or contractors; digital information is only to be stored on password-protected computers using personal LFS login details and must only be stored on LFS-approved systems with enforced access control mechanisms; paper files must not be left unattended at any time and may be collected by designated or relevant staff for safekeeping or to be destroyed safely; paper files must be locked away

				securely when not in use; all records, digital and paper, must always be labelled or otherwise easily identifiable as 'confidential' and, where practicable, protected with a secure password.
Internal Email	Information or data classed as 'public' may be sent internally via email without restrictions.	Information or data classed as 'internal' may be sent internally via email without restrictions, but users are required to ensure information or data is only sent to persons authorised to receive the information as per this policy.	Information or data classed as 'restricted' may be sent internally via email on a need-to-know basis only and users are required to ensure information or data is only sent to persons authorised to receive the information as per this policy.	Information or data classed as 'confidential may be sent internally via email only to designated or relevant members of staff and users are required to ensure information or data is only sent to persons authorised to receive the information as per this policy. Permissions of the email must be set to 'confidential' to ensure full protection of the email and any information or data contained within.
External Email	Information or data classed as 'public' may be sent to third parties via email without restrictions.	Information or data classed as 'internal' or 'restricted' may be sent to third parties via email by authorised members of staff only and only where the third party has a legitimate interest or where there are contractual, statutory, regulatory or otherwise legal obligations. Users are required to ensure information or data is only sent to persons authorised to receive the information as per this policy.		Information or data classed as 'confidential may be sent to third parties via email by designated or authorised relevant members of staff only and only where the third party has a legitimate interest or where there are contractual, statutory, regulatory or otherwise legal obligations. Users are required to ensure

information or data is only sent to persons authorised to receive the information as per this policy. Permissions of the email must be set to ‘confidential’ to ensure full protection of the email and any information or data contained within.

5. Disposal of Data and Information

Any data or records classified as 'Restricted' or 'Confidential' will be disposed of securely and in accordance with any applicable retention schedule. This may include usage of dedicated, secure bins for paper records and securely deleting files from media that may contain such data or records from these categories and securely formatting hard drives.

6. Version Control

Version Number	Changes	Author, Title	Date
0.1	-	Moshe Nitzani, IT Manager	21/05/2018
0.2	Review by Dan Lawson, Acting COO	Dan Lawson, Acting COO	01/06/2018
0.3	Comments by GDPR working group incorporated	Dan Lawson, Acting COO	08/06/2018
0.4	Review by Philip Ramge, Academic Registrar	Philip Ramge, Academic Registrar	08/06/2018
0.5	Comments by GDPR working group added; Section 5 added	Philip Ramge, Academic Registrar	12/06/2018 18/06/2018
0.6	Revisions by Dan Lawson, Acting COO	Dan Lawson, Acting COO	03/07/2018
1.0	Approved by Management Team	-	10/09/2018