Student ICT and Email Policy

Section A

1. Computers, Electronic and the Internet Acceptable Usage

To maximise the benefits of our computer resources and minimise potential liability, you are only permitted to use the School's computer systems in accordance with the following guidelines.

2. General Rules

The School's computer systems and their contents belong to the School, and they are intended for business purposes. You are permitted to use the systems to assist you in performing your job. The School has the right to monitor and access all aspects of its systems, including data which is stored on the School's computer systems. You must receive prior approval before using any computer systems belonging to staff members for personal use.

3. Security

To safeguard the School's computer systems from viruses, you are not permitted to load or run unauthorised software, or modify installed software.

4. Use of the Internet and Email

Messages sent over the e-mail system can give rise to legal action against the School. Claims of defamation, breach of confidentiality or contract could arise from a misuse of the system. It is therefore vital for e-mail messages to be treated like any other form of correspondence. You are also reminded that e-mail messages may be disclosed in any legal action commenced against the School relevant to the issues set out in the e-mail.

The School reserves the right to regularly inspect files stored on the production office computers and to monitor sites visited by you on the Internet, material downloaded or uploaded and any e-mail sent or received, in order to ensure compliance with this policy.

5. Inappropriate Use

Misuse of the School's computer systems may result in disciplinary action, up to and including dismissal. Examples of misuse include, but are not limited to, the following:

Sending, receiving, downloading, displaying or disseminating material that insults, causes offence or harasses others.

Users must not introduce any virus, worm, malware, trojan horse or any other "nuisance" program or file onto any system or take any action to circumvent or modify any precautions taken by the LFS to prevent "infection" of its machines.

Users may only access their own files and files which they have been given express permission to access

Accessing racist or other inappropriate or unlawful materials

Downloading or disseminating copyright materials

Transmitting confidential information about the School or its clients

Users must not allow any password associated with his/her Username to become known to another user. The user will be held responsible for any unlawful action carried out under his/her computer account unless there is evidence to prove otherwise.

Interference with or removal of printout which belongs to another person is not permitted. Uncollected printout will be disposed of.

All electronic forms of communications between staff members, enrolled students, governors, and visiting lecturers must be conducted via the LFS provisioned or approved platforms. The use of private channels of electronic communications for LFS business is prohibited. The LFS will not be held responsible for any communication taking place on non LFS provisioned communication platform between staff, students, and governors.

6. Prevent

The Counter-Terrorism and Security Act 2015 (the Act) introduced a package of measures aimed at countering the risk of terrorism and radicalisation. Part 5 of the Act puts hitherto voluntary elements of the 'Prevent' strategy onto a statutory footing.

Staff and students must be aware that any access to security sensitive websites, visiting websites promoting terrorism, downloading and disseminating such material from the LFS IP addresses, may be interpreted by police as evidence of sympathy or even willingness to collude with terrorism.

If you are a student, please consult your course or personal tutor on this matter.

7. Disclaimers

The LFS accepts no responsibility for the malfunctioning of any equipment or software that results in the failure of security or integrity of any stored program or data.

Student files save on the production office computer are liable to be removed at any given moment, the LFS accepts no responsibility for loss of files as of the result of such action. Please make sure you save your files on your personal cloud storage or media.

Section B
LFS Student Email Policy

8. Introduction

The purpose of this Policy is to set out the conditions under which the LFS email system Office 365 – may be used.

9. Who is this policy for?

It applies to all students or who use the LFS email (@student.lfs.org.uk email addresses or @lfs.org.uk), as well as former students (alumni) who continue to use their accounts.

10. Policy

Following enrolment LFS provides all students with an email account in order to have one dedicated channel of communication with them. The purpose of this Policy is to set out the conditions under which the School's email system –may be used. It applies to all students who use the LFS email account, as well as alumni who may continue to use their accounts for up to 1 (one) year and 1 (one) month from graduation.

Immediately after graduation students will be requested to supply an email address so that we can communicate with them for legitimate interests relating to being an alumni of the London Film School. Graduates can opt out of this at any time.

LFS Graduates will be allowed to continue using IT services such as Office 365 and access to the VLE for one year and one month after the graduation board. Graduates will be informed of the cut-off and date by Registry or IT Department and will receive alerts closer to the date.

11.1. Responsibilities

All users of the LFS email system are responsible for the security of their mailboxes and must not disclose their passwords to others. They are also responsible for all activities that occur within their accounts. If a user becomes aware that any unauthorised access has taken place, he/she should notify helpdesk@lfs.org.uk immediately.

Any emails sent by LFS to students will be delivered to their LFS Office 365 Mail addresses and students must ensure that they check their accounts regularly.

11.2. Ownership

LFS provides all students with an email account for the duration of their studies. They are also permitted to continue to use the email account for up to 1 year and one month after the final decision by the external examiners' board. After this Office 365 account will be deleted completely. All user's data in the cloud will be deleted, that includes LFS Outlook emails and files stored in OneDrive. It is the responsibility of each student to make backup copies of any important files stored in Office 365 before 1 (one) year and 1 (one) month after the final decision by the external examiners' board.

Students should be aware that every email address and associated account – whether used by a current or former student – is the property of LFS. It is therefore important that students and alumni remove all their personal emails and any items of a personal nature that they wish to retain from their LFS Office 365 account in advance of it being closed.

11.3. Personal data

Office 365 and its related applications (e.g. OneDrive, Outlook, Calendar, Microsoft Teams) are hosted in the cloud. Microsoft handles all personal data in line with their privacy policies. .

LFS acts as the domain administrator for Microsoft 365 facilities and administers all email accounts in accordance with its Data Protection Policy (available in the Policy and Regulations section of the website).

11.4. Legislation

Emails and instant messages are subject to the same laws that apply to other forms of communication, including defamation, harassment, copyright and data protection.

11.5 Acceptable use

Authorised users of the LFS email system must use its facilities responsibly, complying with all relevant policies and laws.

11.5.1 Acceptable Use Policy

The policy requires account holders not to: .

- generate or facilitate unsolicited bulk commercial email;
- violate or encourage the violation of the legal rights of others;
- use the services for any unlawful, invasive, infringing, defamatory or fraudulent purpose;
- intentionally distribute viruses, worms, Trojan horses, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- interfere with the use of the services, or the equipment used to provide the services, by customers, authorised resellers, or other authorised users;
- alter, disable, interfere with or circumvent any aspect of the services;
- test or reverse-engineer the services in order to find limitations, vulnerabilities or evade filtering capabilities;
- grant multiple individuals access to an individual End User Account other than via the delegation features provided within the Services;
- create End User Accounts assigned to business functions rather than to human beings for the purpose of sharing files within or outside of the domain;
- resell End User Accounts or parts thereof as added into a commercial product offered to third parties;
- to record audio or video communications without consent if such consent is required by applicable laws and regulations (You are solely responsible for ensuring compliance with all applicable laws and regulations in the relevant jurisdiction(s)).

11.5.2 Prohibited use

The LFS email system must not be used for:

- the creation, transmission or storage of text, images and other material that is offensive, obscene, indecent, discriminatory, harassing or libellous;
- the transmission of material that infringes the intellectual property rights of another person, including copyright;
- the creation or transmission of material that brings LFS into disrepute;
- the incitement of violence;
- activities that corrupt or destroy other users' data or disrupt the work of others;
- activities that violate the privacy of others or unfairly criticise or misrepresent others;
- unauthorised personal financial gain or a commercial or profit-making nature, e.g. trading on eBay.

This list is not exhaustive. Contravention of any of the above terms (listed in sections 2.1 and 2.2) may result in the suspension or termination of a user's Microsoft 365 facilities. The instigation of formal action under the LFS disciplinary procedures may follow and, in certain circumstances, legal action may be taken.

11.6 Security

Students are responsible for the security of their mailboxes and must not disclose their passwords to others. In addition to a strong password, the University requires the use of multifactor authentication (twostep verification) for Microsoft 365 accounts.

Although emails are routinely scanned for virus content and spam, students are expected to take reasonable measures to prevent the introduction and transmission of computer viruses. These include:

- not opening attachments received from unsolicited or untrusted sources;
- not transmitting attachments known to be infected with a virus;
- ensuring that antivirus/anti-spyware software is installed and maintained on any computer used to gain access to the LFS IT facilities.

The unauthorised interception of, or access to, the messages of others is illegal.

The LFS helpdesk should be informed immediately if a suspected virus is received or a user becomes aware that someone has gained unauthorised access to his/her account.

The LFS is using Sophos as the Spam and Phishing filtering system. Sophos will identify most spam and suspicious emails and will automatically remove the vast majority of these. The process is not perfect and some legitimate emails may end up as false positive. Sophos will alert you daily on detected Spam and you will be given the chance to release the false positive email back into your inbox.

Finally, some spam makes it through all security filters and controls and will arrive in your inbox, hence the need to always be vigilant and to challenge any emails that appear suspicious. When this happens, students can teach Microsoft 365 to recognise spam by right clicking the email message and setting the Security Options to Junk, Block or Phishing. This will send the email to your Spam folder and remove it from your inbox, and Microsoft will continue to do the same if you receive future emails from that sender.

11.7 Monitoring

Account activities (e.g. storage usage, number of log-ins etc) are monitored by Microsoft and all messages are routinely scanned (for viruses, spam, and other security threats) to assist with the effective operation of the email system. The University, as the domain administrator for Microsoft's facilities, may use analytical tools to monitor the University's use of Microsoft 365 and have access to information held in an email account. The University reserves the right to access this information in the following circumstances:

- to investigate a complaint, where relevant;
- to investigate a reasonable suspicion of abuse of computer facilities;
- to cooperate in the investigation of a crime;
- in an emergency situation, including as a response to a potential cyber incident.

Otherwise, the University will respect the privacy of all email account holders.

11.8. Storage Limits

Each student is allocated 50GB of email storage and 1TB of OneDrive storage.

12 Managing email accounts

12.1. Email addresses

Each student will be provided with an email account at the time of enrolment. The address for the account will be based on their first and last name. and the information it will contain includes their cohort number and course title.

12. Version Control: Policy

Version Number	Changes	Author, Title	Date
1.0	New student policy	Approved by Academic Board	08/12/2021