THE LONDON
INTERDISCIPLINARY
SCHOOL

IT Acceptable Use Policy

1.0 Purpose

1.1 LIS seeks to promote and facilitate the proper and extensive use of Information Technology (IT) for the sole purpose of supporting the teaching, learning, research and business activities of LIS; as well as for any legal activity that further the aims and policies of LIS.

1.2 Whilst the traditions of academic freedom will be fully respected (see Academic Freedom Policy), this also requires responsible and legal use of the technologies and facilities made available to the learners and staff of LIS.

1.3 It is the responsibility of all Users of LIS's IT services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements. The policy will be officially reviewed on an annual basis.

1.4 This Acceptable Use Policy is intended to provide a framework governing the use of all IT resources. It should be interpreted such that it has the widest application, so as to include new and developing technologies and uses, which may not be explicitly referred to.

2.0 Scope

2.1 This policy applies to all Users including staff, students and visitors. It also addresses the use of LIS's IT facilities accessed via resources not fully owned by LIS, such as the use of personal BYOD ('bring your own device') equipment.

2.2 The IT facilities include hardware, software, data, storage, network access, telephony, printing, back office systems and services and service provided by third parties including online, Cloud and hosted services.

3.0 Definitions of Unacceptable Use

3.1 The LIS network is defined as all computing, telecommunication, and networking facilities provided by LIS, with particular reference to all computing devices, either personal or LIS owned, connected to systems and services supplied on-premises or remotely.

3.2 The conduct of all Users when using LIS's IT facilities should always be in line with the institution's values, including the use of online and social networking platforms.

Unacceptable use includes:

3.3 Creation or transmission, or causing the transmission, of any hateful, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

3.4. Creation or transmission of material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of LIS or a third party or which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation.

3.5. Creation or transmission of material with the intent to defraud or which is likely to deceive a third party or which advocates or promotes any unlawful act.

3.6 Creation or transmission of unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others.

3.7. Creation or transmission of unsolicited or bulk email (spam), forge addresses, or use mailing lists other than for legitimate purposes related to LIS's activities.

3.8. Creation or transmission of material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party.

3.9. Creation or transmission of material that brings LIS into disrepute.

3.10. Deliberate unauthorised access to networked facilities or services or attempts to circumvent College security systems.

3.11 Use of peer-to-peer services and software including but not limited to torrenting, filesharing, and newsgroups.

3.12. Pursuance of commercial activities for personal gain.

3.13. Deliberate activities having, with reasonable likelihood, any of the following characteristics:

- Wasting staff effort or time unnecessarily on IT management.
- Corrupting or destroying other users' data.
- Violating the privacy of other users.
- Disrupting the work of other users.
- Denying service to other users (for example, by deliberate or reckless overloading of access links or switching equipment).
- Continuing to use an item of networking software or hardware after a request that use should cease because it is causing disruption to the correct functioning of the network.
- Other misuse of network resources, such as the introduction of computer viruses, malware, or other harmful software.
- Using LIS systems in part or whole to maliciously breach GDPR rules.
- Introduce data-interception, password-detecting or similar software or devices to LIS's Network.

4.0 Storage

4.1 Storage provided by LIS should not be used to store files larger than 2GB without the prior consent of the Head of Digital. Consent will typically be sought and provided for in the form of dated email correspondence.

4.2 Storage of copyrighted material is expressly forbidden without the prior consent of the Registrar. Consent will typically be sought and provided for in the form of dated email correspondence.

5.0 Monitoring

5.1. Through its property managers, LIS monitors the use of its IT facilities, under the Regulation of Investigatory Powers Act (2000) for the purposes of:

- The effective and efficient planning and operation of the IT facilities;
- Investigation, detection and prevention of infringement of the law, this policy or other LIS policies;
- Investigation of alleged misconduct by staff or students;

5.2. LIS will comply with lawful requests for information from government and law enforcement agencies.

5.3. Users must not attempt to monitor the use of the IT facilities without explicit authority to do so.

5.4. Access to workspaces, email, and/or individual IT usage information will not normally be given to another member of staff unless authorised by the Registrar, or nominee, who will use their discretion, normally in consultation with the Delegated HR Lead.

5.5. Where there is a requirement to access the account of another member of staff, authorisation must be obtained in writing from the Delegated HR Lead.

5.6. If the request for access is related to a HR investigation, this should be managed wholly by the Delegated HR Lead.

5.0 Consequences of Breach of IT Acceptable Use Policy

5.1 In the event of any failure to comply with the conditions of this Acceptable Use Policy by a User, LIS may in its sole discretion:

1. Restrict or terminate a User's right to use LIS's IT facilities.
2. Withdraw or remove any material uploaded by that User in contravention of this Policy.
3. Where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.
4. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with LIS's Disciplinary Policy. Disciplinary action may ultimately lead to dismissal.

6.0 Data breach or data query

6.1 Should there be a suspected data breach, the Registrar - in their role as Data Protection Officer - should be informed immediately via email (registrar@lis.ac.uk).

6.2 Queries relating to the correct application of GDPR rules should be sent to the Registrar in their role as Data Protection Officer (registrar@lis.ac.uk).

7.0 Other legal frameworks

7.1 The use of LIS's IT systems and resources are subject to the following statutes and regulations:

- The Copyright, Designs and Patents Act 1988
- Computer, Copyright Software Amendment Act 1985
- The Computer Misuse Act 1990
- The Data Protection Act 1998
- General Data Protection Regulation (GDPR) (EU) 2016/679
- The Electronic Communications Act 2000
- The Freedom of Information Act 2002
- The Regulation of Investigatory Powers Act 2000
- Trade Marks Act 1994
- Prevent duty guidance: for higher education institutions in England and Wales
- Criminal Justice and Public Order Act 1994

Copies of these documents are available online at http://www.opsi.gov.uk/

Version Control

Name of policy/procedure:	IT ACCEPTABLE USE POLCY
Document owner:	Kestral Gaian, Head of Digital
Date Originally Created:	01/2019
Related documents: (e.g. associated forms, underpinning processes, related policies or overarching policies)	Data Retention Policy Detailed Data Retention Schedule

Version Control		
Author	Date	Brief summary of changes
Michael Englard, Registrar	13/01/2019	Original