**The London School of Jewish Studies (LSJS)**

**LSJS Data Protection, Cyber Security and IT Acceptable Use Policy**

## DATA PROTECTION

### 1. INTERPRETATION

### 1.1 DEFINITIONS:

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. LSJS is the Controller of all Personal Data relating to our Staff and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Officer (DPO): the person with responsibility for data protection compliance.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when LSJS collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal

Staff: all employees, volunteers and others.

UK GDPR: the retained EU law version of the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the UK UK GDPR.

## 2. INTRODUCTION

2.1 This Policy sets out how LSJS ("we", "our", "us ") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

2.2 This Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees,

workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

2.3 This Policy applies to all Staff ("you", "your"). You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements. This Policy sets out what we expect from you for LSJS to comply with applicable law. Your compliance with this Policy is mandatory. Any breach of this Policy may result in disciplinary action.

2.4 This Policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

## 3. SCOPE

3.1 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. LSJS is exposed to potential fines of up to £17.5million for failure to comply with the provisions of the UK GDPR.

3.2 The DPO is responsible for overseeing this Policy. That post is held by Paul Gould, 020 8203 6427 x 205, paul.gould@lsjs.ac.uk

3.3 Please contact the DPO with any questions about the operation of this Policy or the UK GDPR or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by LSJS) (see paragraph 5.1);

(b) if you need to rely on Consent and/or need to capture Explicit Consent (see paragraph 6);

(c) if you need to draft Privacy Notices (see paragraph 7);

(d) if you are unsure about the retention period for the Personal Data being Processed (see paragraph 11);

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see paragraph 12.1);

(f) if there has been a Personal Data Breach (see paragraph 13);

(g) if you are unsure on what basis to transfer Personal Data outside the EEA (see paragraph 14);

(h) if you need any assistance dealing with any rights invoked by a Data Subject (see paragraph 15);

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 19) or plan to use Personal Data for purposes other than what it was collected for;

(j) if you plan to undertake any activities involving Automated Processing (see paragraph 20);

(k) if you need help complying with applicable law when carrying out direct marketing activities (see paragraph 21); or

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see paragraph 22).

## 4. PERSONAL DATA PROTECTION PRINCIPLES

4.1 We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

(a) processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

(b) collected only for specified, explicit and legitimate purposes (Purpose Limitation);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

(d) accurate and where necessary kept up to date (Accuracy);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);

(f) processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);

(g) not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

4.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

## 5. LAWFULNESS, FAIRNESS AND TRANSPARENCY

5.1 Lawfulness and fairness

5.2 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.3 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

5.4 The UK GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests;

(e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices

5.5 The DPO will identify and document the legal ground being relied on for each Processing activity.

## 6. CONSENT

6.1 A Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent.

6.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6.3 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.4 When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

6.5 You will need to evidence Consent captured and keep records of all Consents in accordance with guidance given by the DPO so that LSJS can demonstrate compliance with Consent requirements.

## 7. TRANSPARENCY (notifying Data Subjects)

7.1 The UK GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. The information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

7.2 Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

7.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

7.4 If you are collecting Personal Data from Data Subjects, directly or indirectly, then you must provide Data Subjects with a Privacy Notice as directed by the DPO.

## 8. PURPOSE LIMITATION

8.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

8.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

## 9. DATA MIMIMISATION

9.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

9.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

9.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

## 10. ACCURACY

10.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

10.2 You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data as directed by the DPO.

## 11. STORAGE LIMITATION

11.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

11.2 LSJS will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time.

11.3 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

11.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with guidelines given by the DPO. This includes requiring third parties to delete that data where applicable.

11.5 You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

## 12. SECURITY INTEGRITY AND CONFIDENTIALITY

12.1 Protecting Personal Data

12.2 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

12.3 LSJS will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

12.4 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

12.5 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it;

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed; and

(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

## 13. REPORTING A PERSONAL DATA BREACH

13.1 The UK GDPR requires Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

13.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

13.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO. You should preserve all evidence relating to the potential Personal Data Breach.

## 14. TRANSFER LIMITATION

14.1 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

14.2 You may only transfer Personal Data outside the UK if one of the following conditions applies:

(a) the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

## 15. DATA SUBJECT'S RIGHTS AND REQUESTS

15.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the UK;

(i) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(j) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(k) make a complaint to the supervisory authority;

(l) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format; and

15.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

15.3 You must immediately forward any Data Subject request you receive to the DPO.

## 16. **ACCOUNTABILITY**

16.1 The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

16.2 LSJS must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Policy, Related Policies, Privacy Guidelines or Privacy Notices;

(d) regularly training Staff on the UK GDPR, this Policy, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. LSJS must maintain a record of training attendance by Staff; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

## 17. RECORD – KEEPING

17.1 The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

17.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents as directed by the DPO.

17.3 These records should include, at a minimum, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

## 18. TRAINING AND AUDIT

18.1 We are required to ensure all Staff have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

18.2 You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

18.3 You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

## 19. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

19.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles.

19.2 You must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

19.3 Data controllers must also conduct DPIAs in respect to high-risk Processing.

19.4 You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

(a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(b) automated Processing;

(c) large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and

(d) large scale, systematic monitoring of a publicly accessible area.

19.5 A DPIA must include:

(a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

## 20. DIRECT MARKETING

20.1 We are subject to certain rules and privacy laws when marketing to our customers.

20.2 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

20.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

20.4 A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

## 21. SHARING PERSONAL DATA

21.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

21.2 You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

21.3 You may only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.

21.4 You must comply with any guidelines given by the DPO on sharing data with third parties.

## 22 IT ASSET MANAGEMENT

22.1 Assign all IT hardware and software to a specific LSJS department or person.

22.2 Keep a detailed automated inventory of all hardware and software assets, noting key details like network address, machine name, and software version.

22.3 Use regular scanning to detect unauthorized hardware/software and alert relevant personnel.

## 23 CYBER SECURITY AND IT ACCEPTABLE USE

23.1 Purpose

The purpose of the Cyber Security and IT Acceptable Use Policy is to outline the acceptable use of all IT resources, including computer hardware and software,

network systems, internet access, email systems, and other electronic communication systems, by students, employees, contractors, and third-party service providers at LSJS. This policy aims to protect the integrity, confidentiality, and availability of LSJS IT resources, and to promote responsible and ethical behaviour when using these resources.

23.2 Scope

Members of LSJS and all other users (staff, students, visitors, contractors and others) are bound by the provisions of its policies in addition to this Acceptable Use Policy. We seek to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of learning, teaching, innovation and research to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to students, staff and our partners.

23.3 Acceptable Use

Users are encouraged to use the IT facilities to further the goals and objectives of their work, study or research and in accordance with the Dignity and Respect policy. Subject to all of the following, LSJS permits personal use of the IT facilities with these conditions:

- It does not interfere with the member of staff's work nor the student's study.
- It does not contravene any LSJS policies; and
- It is not excessive in its use of resource

All users of the LSJS IT resources must comply with all applicable laws, regulations, and policies, including but not limited to the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

LSJS has a statutory duty (the Prevent Duty), under Section 26(1) of the Counter Terrorism and Security Act 2015, to act to stop members of its community from being drawn into terrorism. In order to comply with this duty, LSJS reserves the right to monitor or block access to material that might incite extremism, radicalisation or violence. Anyone needing to access security sensitive material for legitimate academic purposes must enquire via the Ethics Review Process.

All users of the LSJS IT resources are responsible for maintaining the security of these resources by using strong passwords, regularly updating software, and reporting any suspicious activity to the IT department.

The LSJS respects the privacy of its users and expects all users to respect the privacy of others. Any unauthorised access, use, or disclosure of personal information is strictly prohibited.

Users must comply with any request made to them by LSJS staff in connection with the enforcement of this policy.

Users shall not use the IT facilities inappropriately. Unacceptable and inappropriate use follows.

23.4 Unacceptable and Inappropriate Use

LSJS IT Systems may not be used directly or indirectly by a User for the download, creation, manipulation, transmission or storage of:

1. any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
2. unlawful material or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others.
3. any material which promotes terrorism or violent extremism, or which seeks to radicalise individuals to such causes.
4. unsolicited and unauthorised bulk email (spam) which is unrelated to the legitimate business of LSJS. For the surveying of students, please refer to the protocol.
5. material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of LSJS or a third party.
6. material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation.
7. material with the intent to defraud or which is likely to deceive a third party.
8. material which advocates or promotes any unlawful act.
9. 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; or
10. material that brings LSJS into disrepute.

LSJS networks must not be deliberately used by a User for activities having, or likely to have, any of the following characteristics:

1. Accessing or attempting to access unauthorised information or resources.
2. Sharing passwords or other access credentials with others.
3. Intentionally wasting staff effort or other LSJS resources.
4. Corrupting, altering or destroying another User’s data without their consent.
5. Disrupting the work of other Users or the correct functioning of LSJS IT systems.
6. Engaging in any activity that may disrupt or interfere with the normal operation of LSJS IT resources.
7. Denying access to LSJS IT Systems and its services to other users.

8. Introduce data-interception, password-detecting or similar software or devices to the LSJS Network.
9. Deliberate unauthorised access to LSJS IT systems.
10. Attempting to undermine the security of the LSJS IT systems.
11. Intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.
12. Installing or using unauthorised software or hardware.
13. Using software which is only licensed for limited purposes for other purpose or otherwise breaching software licensing agreements.
14. Failing to comply with a request from an authorised person for you to change your password.

The LSJS email system and instant messaging system are intended for LSJS-related activities only. It is recommended to use clear and concise language when composing messages and avoid sending large attachments or forwarding chain emails.

All users of the LSJS email system should not:

- harass, threaten, or intimidate others.
- solicit or promote personal or personal commercial activities.
- send confidential or sensitive information without using appropriate encryption methods.

LSJS recognises the value of social media as a communication and engagement tool. Use social media in a responsible and ethical manner.

All users of social media accounts representing as a member of LSJS should not:

- post offensive or inappropriate content, including but not limited to sexually explicit or discriminatory material.
- harass, threaten, or intimidate others.
- promote personal or commercial activities without prior approval from LSJS.

Any unauthorised use of IT resources may result in disciplinary action, up to and including termination of employment or contractual relationship.

Where the LSJS networks are being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the LSJS networks.

23.5 Consequences of Breach

In the event of a breach of this Acceptable Use Policy by a User, LSJS may at its discretion:

- restrict or terminate a User's right to use the LSJS network and systems.
- withdraw or remove any material uploaded by that User in contravention of this Policy.
- 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.

In addition, where the User is also a member of the LSJS community, we may take such action, disciplinary or otherwise as it deems appropriate, and which is in accordance with its Charter, Statute, Ordinances and Regulations.

**24 PREVENT**

24.1 LSJS has a statutory duty (the Precent Duty) under Section 26 (1) of the CounterTerrorism and Security Act 2015, to act to stop members of its community from being drawn into terrorism. In order to comply with this duty, LSJS reserves the right to monitor or block access to material that might incite extremism, radicalisation or violence. Anyone needing to access security sensitive material for legitimate academic purposes must enquire via the Ethics Review Process.

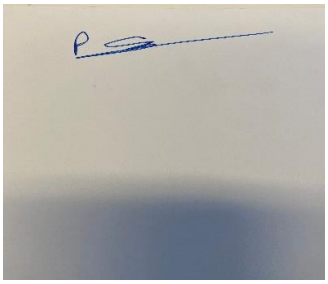
24.2 All users of the LSJS IT resources are responsible for maintaining the security of these resources by using strong passwords, regularly updating software, and reporting any suspicious activity to the IT department.

24.3 The LSJS respects the privacy of its users and expects all users to respect the privacy of others. Any unauthorised access, use, or disclosure of personal information is strictly prohibited.

24.4 Users must comply with any request made to them by LSJS staff in connection with the enforcement of this policy.

24.5 Users shall not use the IT facilities inappropriately. Unacceptable and inappropriate use follows.

Signed on behalf of LSJS:



(Paul Gould, on behalf of senior leadership team, LSJS).

Date: August 2023

To be reviewed in August 2025