S P Jain London School of Management	**Data Protection Policy**
Document Type	Policy
Administering Entity	Chief Operating Officer, Heads of Services, all staff
Latest Approval/ Amendment Date	25/05/2023
Approval Authority	Board of Directors

1. Purpose

a) The purpose of the Data Protection Policy is to clarify the requirements under Data Protection legislation in the context of the S P Jain London School of Management (the School). It aims to clarify the responsibilities and duties of staff and to set out the structure for compliance with data protection legislation.

2. Scope

a) This policy applies to the processing of personal data by members of the School or on behalf of the School.

b) Processing" encompasses the collection, recording, structuring, storage, adaptation or alteration, retrieval, use, making available, alignment or combination, restriction, erasure or destruction of personal data by either manual or automated means.

c) "Personal data" encompasses any information relating to a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person and, therefore, this Policy applies to anything which is recorded in relation to an individual.

3. Relationship with existing policies

a) This policy should be read in conjunction with IT and Information Security policies, CCTV policy and the Records Management Policy.

4. Policy statement

a) The School is committed to the protection of individuals' rights and privacy. The processing of personal data such as the collection, recording, use, and storage of personal information must be dealt with lawfully and correctly in accordance with this policy. All information and systems containing personal data must be protected against unauthorised access, accidental loss or destruction, modification or disclosure.

b) The School regards the lawful and correct treatment of personal data as important to its successful operation, and to maintain confidence with our students and staff and other stakeholders. The School shall, therefore, at all times act in a manner consistent with the

obligations of a Data Controller under the provisions of Data Protection legislation ensuring privacy is a key consideration in its operations and that individuals' rights under the legislation are respected.

c) All members of the School who handle or have access to Personal Data under the control of, or on behalf of, the School must comply with this Policy.

5. Data Protection Principles

a) The data protection legislation sets out the main principles for organisations when processing data and the School must ensure that personal data is:

i) processed lawfully, fairly and in a transparent manner in relation to individuals;
ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
iii) further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
iv) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
v) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without dela
vi) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
vii) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6) Lawful basis for processing

a) The processing must be on one of the following legal bases:

Consent: the individual has given clear consent to process their personal data for a specific purpose.

Contract: the processing is necessary for a contract with the individual, or because they have asked the School to take specific steps before entering into a contract.

Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).

Vital interests: the processing is necessary to protect someone's life.

Public task: the processing is necessary to perform a task in the public interest or for your official functions, and the task or function has a clear basis in.

Legitimate interests: the processing is necessary for the School's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply when the School is processing data to perform its official tasks).

b) In addition to having one of the lawful bases outlined above, the processing must also be necessary. Where the School is using legitimate interests as the basis for processing, this will be documented in a Legitimate Interests Assessment.

7) Special Category data

a) In order to process special category data, the School must also ensure that one of the following also applies as well as one of the legal bases outlined in paragraph 6 above;

i) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
ii) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection;
iii) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
iv) processing relates to personal data which are manifestly made public by the data subject;
v) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
vi) processing is necessary for reasons of substantial public interest, on the basis of UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
vii) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or UK law or pursuant to contract with a health professional;
viii) processing is necessary for reasons of public interest in the area of public health;
ix) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on EU or UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

b) The Legislation also sets out the requirements for processing criminal convictions and the particular safeguards which need to be in place. Where the School is processing criminal convictions, it must ensure that it has identified a lawful basis as for special category data above. In addition to determining a lawful basis, the School must also document its procedures for processing criminal convictions in an appropriate policy. These are as follows:
i) the processing criminal conviction data for applicants and students who are not on courses leading to professional registration is subject to the Policy for the consideration of applicants and students with a criminal conviction;
ii) the processing criminal conviction data for job candidates and staff is subject to the Staff Policy and Procedure for Criminal Convictions.

8) The rights of the individual

a) The School must respect individuals' rights when processing personal data. These are enshrined in the legislation as follows:

i)	The right to be informed
ii)	The right of access
iii)	The right to rectification
iv)	The right to erasure
v)	The right to restrict processing
vi)	The right to data portability
vii)	The right to object
viii)	Rights in relation to automated decision making and profiling

b) The rights above depend upon the lawful basis for processing. For example, the right to erasure only applies where the lawful basis for processing is consent. Where public task, legitimate interests, contractual basis or a legal requirement are used as the basis for processing, the right of rectification, restriction and the right to object are also limited to ensuring that the data is accurate before it can be processed.

c) The right to be informed is, however, a key right and applies in all circumstances (see Transparency below).

9) Data protection by default

a) Where the School is undertaking new processing (e.g. it is collecting a new type of data or it is implementing a new system or process), it must consider building in data protection from the outset, including the organisational and technical measures to ensure appropriate security.

b) This may include undertaking a Data Protection Impact Assessment (DPIA) which is required for significant processing and where there are significant risks. Where a DPIA is not required, the School must still consider the risks to the individual of processing and how these risks will be mitigated and to document this assessment.

10) Data minimisation

a) Under GDPR, the School has an obligation to ensure that it collects only what data is necessary. Those who are collecting data should, therefore, ensure that it is limited to what is required.

11) Transparency

a) The School needs to provide specific information to people about how it processes their personal data. To provide this information, the School must provide a privacy notice. The Privacy Notices must be published on the School website and made available to the data subjects.

b) In addition to the privacy notices, the School is also required to inform data subjects of the purposes and use of data at the point of collection. Any School forms (whether paper-based or web-based) that gather data on an individual should contain a statement on why data is being gathered and how it will be used.

12) Staff Responsibilities for data protection

a) The Senior Management Team are responsible for data protection as a whole and in their areas of responsibility and they must seek assurance that members of their teams implementing the Data Protection Policy as appropriate.

b) The Chief Operating Officer is the appointed Data Protection Officer responsible for the management of data protection matters and for the development of specific guidance and practice on data protection issues for the School. The tasks of the DPO are as follows:

i) to inform and advise the School and its employees about their obligations to comply with the GDPR and other data protection laws:
ii) to monitor compliance with the GDPR and other data protection laws, and with the School's data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits
iii) to advise on, and to monitor, data protection impact assessments
iv) to cooperate with the supervisory authority; and
v) to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, students etc).

c) Heads of Service are responsible for developing and maintaining good information handling practice within the School in accordance with this Policy. They must

i) maintain accurate records of the data processed in their department in accordance with the requirements of this policy and the Records Management Policy.
ii) ensure that individuals are clear about what data the School holds through an appropriate Privacy Notice;
iii) ensure that all staff are trained in Data Protection and are aware of their responsibilities
iv) ensure that all data is kept securely and that any breaches are notified immediately.

d) All staff or others who process personal data must ensure that they understand their obligations under this Policy and how to protect personal data.

e) Where staff undertake research which involves personal data, they must ensure that it is carried out with reference to Data Protection and ethical guidelines

f) All staff are responsible for reporting any breach or potential incident, likely to result in unauthorised disclosure, damage, destruction or loss of Personal Data directly to the Chief Operating Officer.

g) Staff must not disclose personal data to a third party except in limited cases where there is a legal or statutory duty to do so or where it is in an individual's vital interests. All staff must therefore take care to ensure that personal data is not disclosed to unauthorised third parties which includes family members of the data subject, friends, government bodies and the Police in certain circumstances without the data subject's consent or the approval of the Chief Operating Officer.

13) Data Protection Training

a) It is mandatory for staff to undertake Data Protection Training. On-line E Learning Data Protection training will be provided at induction. Staff in key roles will be provided with additional Data Protection training as required by their role.

14) Security

a) The School must ensure that it has appropriate technical and organisational measures in place to ensure the security of personal data and these are documented in its IT policies.

b) All staff are responsible for ensuring personal data are kept securely and accessible only to those who need to use it. Appropriate security measures are to be taken to prevent accidental loss of, or damage to, personal data. This will mean the use of passwords or encryption for electronic documents and keeping papers under lock and key**.**

15) Breaches

a) All breaches of data protection should be reported to the Chief Operating Officer immediately. An assessment will be made as to whether there are significant risks to the rights and freedoms of individuals and whether a notification must be made to the Information Commissioner's Office. Any such notification must be approved by the Chief Operating Officer and reported within 72 hours of the notification of the breach.

16) Right of access

a) Staff, students and other data subjects about whom the University holds or uses personal data have a legal right to access that information and request a copy of the data in permanent form. Any person wishing to exercise their right of access formally should complete the "Data Subject Access Form" and submit it along with evidence of proof of identity to prevent unlawful disclosure of personal data to the Chief Operating Officer.