LONDON SCHOOL OF BUSINESS AND MANAGEMENT STUDIES

DATAPROTECTIONPOLICY
&
PROCEDURES

Contents

1 POLICY STATEMENT

London School of Business and Management Studies (*hereinafter referred to as the* ***"School"****)* needs to collect personal information to effectively carry out our everyday business functions and activities. Such data is collected from staff and students.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however, we are committed to processing all personal information in accordance with the ***General Data Protection Regulation (GDPR)***, ***UK data protection laws*** and any other relevant the data protection laws and codes of conduct *(herein collectively referred to as* ***"the data protection laws"****).*

The School has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles.

2 PURPOSE

The purpose of this policy is to ensure that the School meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and, in the individuals, best interest.

The data protection laws include provisions that promote accountability and governance and as such the School has put policies and procedures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third parties on the responsibilities of handling and accessing personal data and data subject requests.

3 SCOPE

This policy applies to those staff members who are dealing with personal data within the School. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

3.1 DEFINITIONS

- ***"Biometric data"*** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.
- ***"Consent"*** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- ***"Data controller"*** means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

- ***"Data processor"*** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- ***"Data protection laws"*** means for the purposes of this document, the collective description of the GDPR, Data Protection Bill and any other relevant data protection laws that the School complies with.
- ***"Data subject"*** means an individual who is the subject of personal data
- ***"GDPR"*** means the *General Data Protection Regulation (EU) (2016/679)*
- ***"Personal data"*** means any information relating to an identified or identifiable natural person *('data subject'*); an identifiable natural person is one 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- ***"Processing"*** means any operation or set of operations performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- ***"Profiling"*** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- ***"Recipient"*** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- ***"Supervisory Authority"*** means an independent public authority which is established by a Member State
- ***"Third Party"*** means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

3.2 GENERAL DATA PROTECTION REGULATION (GDPR)

The ***General Data Protection Regulation (GDPR) (EU) 2016/679)*** was approved by the European Commission in April 2016 and will apply to all EU Member States from 25th May 2018. As a *'Regulation*' rather than a *'Directive'*, its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As the School processes personal information regarding individuals (*data subjects*), we are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

3.2.1 PERSONAL DATA

Information protected under the GDPR is known as *"personal data"* and is defined as: -

"Any information relating to an identified or identifiable natural person; an identifiable natural person is one 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

The School ensures that a high level of care is afforded to personal data falling within the GDPR's **'special categories'** *(previously **sensitive personal data***), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

3.2.2 THE GDPR PRINCIPLES

Article 5 of the GDPR requires that personal data shall be: -

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ***('lawfulness, fairness and transparency')***

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ***('purpose limitation')***

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimisation')***

d) 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 delay ***('accuracy')***

e) 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation')***

f) 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 ***('integrity and confidentiality').***

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles'* ***('accountability')*** and requires that firms ***show***

how they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

3.3 THE INFORMATION COMMISSIONERS OFFICE (ICO)

The Information Commissioners Office (ICO) is an independent regulatory office who report directly to Parliament and whose role it is to uphold information rights in the public interest. The legislation they have oversight for includes: -

- The Data Protection Act 1998*(pre-25th May 2018)*
- General Data Protection Regulation *(post-25th May 2018)*
- The Privacy and Electronic Communication (EU Directive) Regulations 2003
- Freedom of Information Act 2000
- The Environmental Information Regulations 2004

The ICO's mission statement is *"to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals"* and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.

Under the data protection laws the ICO, as the UK's data protection authority (*Supervisory Authority*), will have a similar role as previously, when it comes to oversight, enforcement and responding to complaints with regards to the data protection laws and those firms located solely in the UK.

3.4 DATA PROTECTION OFFICER

Articles 37-39, and Recital 97 of the GDPR detail the obligations, requirements and responsibilities on firms to appoint a Data Protection Officer and specifies the duties that the officer themselves must perform.

A Data Protection Officer (DPO) must be appointed by a firm where: -

- The processing is carried out by a public authority or body *(except for courts acting in their judicial capacity)*
- the core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
- the core activities of the controller/processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10

The College has appointed a designated **DPO,** in accordance with the GDPR requirements and have ensured that the assigned person has an adequate and expert knowledge of data protection law.

For the DPO duties and responsibilities please refer to our DPO Responsibilities document.

4 GOVERNANCE PROCEDURES

4.1 ACCOUNTABILITY & COMPLIANCE

LSBS has implemented appropriate measures to ensure the safeguarding of personal data and compliance with the data protection laws and can evidence such measures through our documentation and practices.

Our main objectives are to: -

- Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance
- Allocate responsibility for data protection compliance

The technical and organisational measures that the School has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct are detailed in this document and associated policies.

4.1.1 DATA MINIMISATION

Under Article 5 of the GDPR, principle (c) advises that data should be *'limited to what is necessary'*, which forms the basis of our minimalist approach. We only ever obtain, retain, process and share the data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Measures to ensure that only the necessary data is collected includes: -

- Electronic collection *(i.e. forms, website, surveys etc)* only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include *'optional'* fields, as optional denotes that it is not necessary to obtain
- Physical collection *(i.e. face-to-face, telephone etc)* is supported using internal forms where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected
- Forms, contact pages and any documents used to collect personal information are reviewed every 12 months to ensure they are fit for purpose and only obtaining necessary personal information in relation to the legal basis being relied on and the purpose of processing

4.1.2 ENCRYPTION

We utilise encryption as a further risk prevention measure for securing the personal data that we hold. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

We utilise encryption via secret key for transferring personal data to any external party and provide the secret key in a separate format. Where special category information is being transferred and/or disclosed, the Data Protection Officer is required to authorise the transfer and review the encryption method for compliance and accuracy.

4.1.3 RESTRICTION

Restricting access is built into the foundation of the School's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose have access to personal information.

4.1.4 INFORMATION AUDIT

To enable the School to fully prepare for and comply with the data protection laws, we have carried out a school-wide data protection information audit to better enable us to record, categorise and protect the personal data that we hold and process.

The audit has identified, categorised and recorded all personal information obtained, processed and shared by our college in our capacity as a controller and has been compiled on a central register which includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Disclosures and Transfers (if applicable)

4.2 LEGAL BASIS FOR PROCESSING *(LAWFULNESS)*

At the core of all personal information processing activities undertaken by the School, is the assurance and verification that we are complying with Article 6 of the GDPR and our lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

4.2.1 PROCESSING SPECIAL CATEGORY DATA

Special categories of Personal Data are defined in the data protection laws as: -

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.

Where the College processes any personal information classed as special category, we do so in accordance with Article 9 of the GDPR regulations and in compliance with the Data Protection Bill's Schedule 1 Parts 1, 2, 3 & 4 conditions and requirements.

We will only ever process special category data where: -

- The data subject has given explicit consent to the processing of the personal data
- Processing is necessary for the purposes of carrying out the obligations of the controller

4.2.2 RECORDS OF PROCESSING ACTIVITIES

The School does not maintain records of processing activities. However, we continually review all such activities to ensure that we will be to record such information as detailed in GDPR Article 30.

4.3 DATA RETENTION & DISPOSAL

The School has defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects *(e.g. shredding, disposal as confidential waste, secure electronic deletion)* and prioritises the protection of the personal data in all instances.

4.3.1 DESTRUCTION AND DISPOSAL OF RECORDS & DATA

All information of a confidential or sensitive nature on paper, card or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our staff and students.

The School is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner.

4.3.2 PAPER RECORDS

Due to the nature of our business, the School retains paper based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential and compliant manner. The School utilise **Onsite-Shredding** to dispose of all paper materials.

4.3.3 ELECTRONIC & IT RECORDS AND SYSTEMS

The School uses computers and technology equipment in the running of our business. From time to time, such assets must be disposed of and due to the information held on these whilst they are active; this disposal is handled in an ethical and secure manner.

The deletion of electronic records must be organised in conjunction with the IT Department who will ensure the removal of all data from the medium so that it cannot be reconstructed.

Only the IT Department can authorise the disposal of any IT equipment. Where possible, information is wiped from the equipment through use of software and formatting.

4.3.4 ERASURE

In specific circumstances, data subjects' have the right to request that their personal data is erased, however the College recognise that this is not an absolute *'right to be forgotten'*. Data subjects only have a right to have personal data erased and to prevent processing if one of the *below conditions applies: -*

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data must be erased in order to comply with a legal obligation

Where one of the above conditions applies and the School received a request to erase data, we first ensure that no other legal obligation or legitimate interest applies. If we are confident that the data subject has the right to have their data erased, this is carried out by the Data Protection Officer in conjunction with any department manager to ensure that all data relating to that individual has been erased.

5 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

The School does not currently carry out any processing activities that are defined as requiring a DPIA; however, we continually monitor all activities against the GDPR Article 35 requirements.

6 DATA SUBJECT RIGHTS PROCEDURES

6.1 CONSENT & THE RIGHT TO BE INFORMED

The collection of personal and special category data is a fundamental part of the products/services offered by the School and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws.

Where processing is based on consent, the College have reviewed and revised all consent mechanisms to ensure that: -

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms
- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes

- Consent is always given by a statement or a clear affirmative action (*positive opt-in*) which signifies agreement to the processing of personal data
- Pre-ticked, opt-in boxes are **never** used
- We have ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through multiple options, including: -
    - Opt-out links in mailings or electronic communications
    - Ability to opt-out verbally, in writing or by email
- Consent withdrawal requests are processed immediately and without detriment
- For special category data, the consent obtained is explicit *(stated clearly and in detail, leaving no room for confusion or doubt*) with the processing purpose(s) always being specified

6.1.1 INFORMATION PROVISIONS

Where personal data is obtained directly from the individual *(i.e. through consent, by employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc*)), we provide the below information in all instances, **in the form of a privacy notice: -**

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The contact details of our data protection officer
- The purpose(s) of the processing for which the personal information is intended
- The legal basis for the processing
- The recipients or categories of recipients of the personal data *(if applicable)*
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with the Supervisory Authority
- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

6.2 PRIVACY NOTICE

The School defines a Privacy Notice as a document that is provided to individuals at the time we collect their personal *data*. We have a link to our Privacy Notice on our website and provide a copy of physical and digital formats upon request. The notice is the customer facing policy that provides the legal information on how we handle process and disclose personal information.

6.2.1 EMPLOYEE PERSONAL DATA

As per the data protection law guidelines, we do not use consent as a legal basis for obtaining or processing employee personal information.

All employees are provided with our Staff Handbook which informs them of their rights under the data protection laws and how to exercise these rights and are provided with a Privacy Notice specific to the personal information we collect and process about them.

6.3 THE RIGHT OF ACCESS

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13/14 and any communication under Articles 15 to 22 and 34 *(collectively, The Rights of Data Subjects*), in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity *(i.e. verbally, electronic*).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

6.3.1 SUBJECT ACCESS REQUEST

Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with: -

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority

Subject Access Requests (SAR) are passed to the **Data Protection Officer** as soon as received and a record of the request is noted. The type of personal data held about the individual is checked against our Information Audit to see what format it is held in, who else has it has been shared with and any

specific timeframes for access.

SARs are always completed within 30-days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

6.4 DATA PORTABILITY

The School provides all personal information pertaining to the data subject to them on request and in a format that is easy to disclose and read. We ensure that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

6.5 RECTIFICATION & ERASURE

6.5.1 CORRECTING INACCURATE OR INCOMPLETE DATA

Pursuant to Article 5(d), all data held and processed by the School is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller informs us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The **Data Protection Officer** is notified of the data subjects request to update personal data and are responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, we add an addendum or supplementary statement where applicable.

Where notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority.

6.5.2 THE RIGHT TO ERASURE

Also, known as *'The Right to be Forgotten'*, the College complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by the School is categorized when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

7 OVERSIGHT PROCEDURES

7.1 SECURITY & BREACH MANAGEMENT

The School ensures the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our ***Information Security Policies*** provide the detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

Whilst every effort and measure are taken to reduce the risk of data breaches, the College has controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

8 TRANSFERS & DATA SHARING

Personal data in the European Union is protected by the General Data Protection Regulation (GDPR) but some other countries may not necessarily have the same high standard of protection for your personal data. **Empire College London** does not transfer or store any personal data outside the EU.

9 MONITORING & RESPONSIBILITIES

The School has appointed a **Data Protection Officer** whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and senior management and to actively stay informed and up-to-date with all legislation and changes relating to data protection. The Data Protection Officer has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place to the Senior Management Team where applicable.