GDPR Policy
Summary of Arrangements

GDPR-1-003

Responsible post holder	Jennifer Pharo
Approved by / on	Group Executive
Next Review	June 2019
Relationship to Strategic Goal	Goal 3 - Investing in Excellence
Publication Method	SharePoint

CONTENTS

1. Introduction

LSEEG has a number of arrangements in place to manage GDPR risks. This policy provides a summary of those arrangements.

2. Scope

The scope of these protocols and procedures covers all corporations currently within the LSEEG Group.

3. Policy Accountabilities

3.1 **The Principles of GDPR** state that personal data shall be

- Processed fairly and lawfully
- Collected to specified, explicit, and legitimate purposes
- Adequate, relevant and limited as to what is necessary
- Accurate and where necessary kept up to date.
- Kept for no longer than is necessary
- Processed in a manner that ensures appropriate security.

3.2 **Our approach to accountability for managing personal data are**

As a public body processing personal data we will appoint a Data Protection Officer
The DPO will have a degree of independence with direct access to the highest management, bound by confidentiality, data subjects will have clear access to the DPO.

The DPO will inform and advise, monitor compliance, provide advice with regard to DPIAs, cooperate and liaise with supervisory bodies, be a point of contact for data subjects.

We will appoint Data Controllers/Champions within the LSEE Group.
Data Controllers/Champions will be specialist managers within the defined areas of data processing activity.

The Data Controllers/Champions will be responsible for implementing appropriate technical and organisational measures and controls, implementing data protection policies, and adhering to codes of conduct to demonstrate compliance.
.
We will provide continuous data protection training and awareness to all staff and managers throughout the LSEE Group.

We will provide and support an environment that maintains a clear desk policies, safe and secure filing and storage of documents, both paper and electronic, restrict the use of mobile storage e.g. pen drives, and provide adequate IT Security and compliant procedures on access to data systems and business applications.

3.3 Processing Activities

These will be monitored for compliance by Data Controllers/Champions who will implement the appropriate technical and organisational measures to ensure that only data necessary for each specific purpose is processed. This obligation applies to the following

- The amount of data collected
- The extent of the processing
- The period of storage
- The accessibility of the data

3.4 Working with Partners and Suppliers

We will ensure that when working with Partners and Suppliers data is only shared with the explicit permission of the data subject.

Data sharing agreements with third party agencies will be endorsed.

The Monitoring and compliance of suppliers and supplier systems will be regularly reviewed to ensure continuous safeguarding and security of personal data

3.5 Proactive management of data protection risk

The Data Protection Officer and Data Controllers are responsible for ensuring risk management controls are in place as follows

Each area is responsible for the identification and resolution of risks in the area it controls.

In the event of a breach, Data Controllers/Champions are responsible for ensuring all breaches are notified to the DPO within 24 hours.

Individual policies specify how risks are managed and how risk management processes work e.g. Social Media, IT Security, and Safeguarding.

General risk assessments covering data processing across all client groups will be completed as Data Impact Assessments where processing is likely to result in high risk to the rights and freedoms of natural persons.

Monitoring or risk through risk register

Management review of data breaches, recorded on breach register

DPIAs completed through GPDR committee, with feedback into the risk management process.

A document management system will support good retention and disposal of personal data held electronically. Transfer of paper information to electronic records will

Our approach to psedonomisation and encryption has been enhanced with the purchase of egress system to ensure safe transfer of personal data.

4. Associated Policies

Everyone has rights with regard to how their personal information is handled. During the course of the College's normal activities we will collect, store and process personal information about our staff and students, recognising the need to treat this in an appropriate and lawful manner.

The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, customers, learners and others with whom we communicate. Information held by the College either electronically or on paper is subject to certain legal safeguards specified in the Data Protection Act 1998 and Subject Access Code of Practice. The Act imposes restrictions on how we may use that information.

Whilst this policy does not form part of any employee's contract of employment or student's contract for services, any breach of this policy will be taken seriously and may result in disciplinary action.

The GDPR policy and associated policies, have been prepared taking account of prevailing legislation and legislation requirements and follows best practice by enabling LSEEG to demonstrate a fair, equitable and transparent environment. Accordingly, the policy has been subject to an Equality Impact Assessment and is suitable for publication under the Freedom of Information Act 2000.

This policy sets out the rules on GDPR and data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of all personal information gathered by LSEEG along with respecting the rights of the data subject to privacy, erasure and security..

The Data Protection Officer and Data Controllers/Champions are responsible for ensuring compliance with this policy and all associated policies.

If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with your line manager, the Data Protection Officer or Data Controller/Champion within your area

4.1 Definitions

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual

(such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

Processing is any activity that involves use of the 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 transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4.2 Privacy

A published privacy statement and policy outlining what personal data we hold and process and the lawful basis upon which we collect and process this information, is detailed in the Privacy statement and policy displayed on the websites of all institutions within the LSEE Group. This statement also provides details of the data subject's rights and the organisational and institutions we have a lawful basis to share personal data.

4.3 Processing

GDPR is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

The data subject is entitled to be:

- Told whether any personal data is being processed
- Given a description of the personal data, the reasons it is being processed and whether it will be given to any other organisations or people
- Given a copy of the personal data;
- Given details of the source of the data (where it is available)

For personal data to be processed lawfully, certain conditions have to be met. These include requirements that the data subject has explicitly consented to the processing, or that the

processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed.

When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

4.3 Accuracy

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

4.4 Retention

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. Details of how long we lawfully keep personal data is outlined in the Archiving and Document Retention policy.

5. Data Subject’s Rights and Privacy

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any data held about them by a data controller
- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

There may be circumstances where data is legitimately disclosed to third parties for the prevention or detection of crime, in accordance with the exemptions permitted in the GPDR and Data Protection Act. Where these circumstances arise, the college will keep a record of the requests made and the responses which are given.

6. Data Security

We will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

GDPR requires LSEEG to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures include:

- Entry controls. Any stranger seen in entry-controlled areas should be reported.
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential).
- Methods of disposal. Paper documents containing personal data should be shredded. Data memory devices e.g. USB memory sticks should have restricted use and be physically destroyed when they are no longer required.
- Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they either log off or ‘lock’ their PC when it is left unattended.

7. DPIAs

All areas of LSECs operations will be covered where data and information is being processed, shared, retained or removed. DPIAs will be standardised across all client groups and sites and follow a simple process as outlined by the ICO.

DPIAs will be conducted when implemented new systems and processes, with management restructure or when new organisations join the LSEE Group.

DPIAs will be produced where the environment or activity varies greatly from the norm egg Staff Recruitment Fairs, Marketing Roadshows, etc.

DPIA templates will be made available to staff and students via the GDPR SharePoint and hardcopy where appropriate.

8. Subject Access Requests

A formal request from a data subject for information that we hold about them should be made using the subject access form available on all the websites of all institutions within the LSEE Group. On completion the form will be submitted to the GDPR@lsec.ac.uk.

Any member of staff who receives a written request should forward it to the Data Protection Officer immediately.

Please refer to the Data Protection: Subject Access Request procedure below.

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. Any information requests should be directed to using the Subject Access Request form on the website.

APPENDIX A

SUBJECT ACCESS REQUEST PROCEDURE

INTRODUCTION

LSEEG is legally obliged to collate and retain certain information about its employees, students and other users for a number of reasons, including monitoring performance, achievements and health and safety. It is also necessary to process information so that staff can be recruited and remunerated, courses organised and legal obligations to funding bodies and other government bodies complied with. To comply with the law, information must be collected, used fairly, stored safely and not disclosed to any other person unlawfully.

To do this, LSEEG must comply with the GDPR Principles as defined above,

All LSEEG staff or others who process or use any personal information must ensure that they follow these principles at all times.

In order to ensure that this happens, LSEEG has developed a Group GDPR Policy of which this procedure forms part.

The College is not obliged to comply with identical or similar requests received from the same individual, unless a reasonable interval has lapsed between the first request and any subsequent ones.

NOTIFICATION OF DATA HELD AND PROCESSED

All staff, students and other users are entitled to:

- Know what personal information LSEEG holds and processes about them and
- Given a description of the personal data, the purpose of processing and the recipients or classes of recipients
- Given details of the source of personal data.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what LSEEG is doing to comply with its obligations under GDPR.

LSEEG will provide all staff with a standard form of notification or privacy statement

This will state the types of data LSEEG holds and processes about them and the reasons for which it is processed.

RESPONSIBILITIES OF STAFF

All staff are responsible for:

- Checking that any information they provide to organisations within LSEEG in connection with their employment is accurate and up to date.
- Inform their local organisation within LSEEG of any changes to information, which they have provided i.e. changes of address. This can be completed through self-service on iTrent.
- Check and monitor personal information held on the central HRIS system iTrent, any information thatLSEEG may send out from time to time,
- Inform LSEEG of any errors or changes.
- If and when, as part of their responsibilities, staff collect information about other people (e.g. about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff, which are attached as Appendix 1.

RIGHTS TO ACCESS INFORMATION

Staff, students and other users of LSEEG have the right to access any personal data that is being kept about them either on computer or in certain structured files and filing systems.

Any person who wishes to exercise this right should complete the Subject Access Request form accessed via website of all institutions within the LSEE Group.
Completed Subject Access Requests should be submitted to the GDPR@lsec.ac.uk

Individuals are entitled to request access to their own, personal data and not to information relating to other individuals (unless they are acting on behalf of that individual).

In some cases, it will be appropriate and reasonable to ask the person making the request to verify their identity unless the identity of the requester is known.

LSEEG aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days of receipt of the Subject Access Request.

SUBJECT CONSENT

Where LSEEG has a lawful basis to process personal data, consent of the individual is not required, in some cases, if the data is sensitive, express consent may be required.

Agreement to enable LSEEG to process some specified classes of personal data is a condition of acceptance of enrolment as a student onto any course and as a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs or courses will bring the data subject into contact with children and young people. LSEEG has a duty under the Children's Act and other enactments to ensure that staff are suitable for the job, and students for the courses offered.

LSEEG also has a duty of care to all staff and students and must therefore make sure that employees and those who use LSEEG facilities do not pose a threat or danger to other users.

LSEEG may seek to obtain information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. LSEEG will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

PROCESSING SENSITIVE INFORMATION

Sometimes it is necessary to process the information about a person's health, criminal convictions, race and gender and family details. This may be to ensure that LSEEG is a safe place for everyone, or to operate other associated LSEEG policies, such as the Managing Sickness Absence Policy.

LSEEG will process sensitive data in order to provide anonymised statistical data for governors or external bodies where compliance is mandatory e.g. DfE.

However, because this information is considered sensitive and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for LSEEG to do this as part of their contract of employment.

Offers of employment or course places may be withdrawn if an individual refuses to consent to this.

Details of all aspects of a data subject's privacy is detailed in the Privacy Statement and Policy published on the LSEEG institutions websites.

APPENDIX B

DATA PROTECTION OFFICER AND THE DESIGNATED DATA CONTROLLERS/CHAMPIONS

The following post holders, as the LSEEG Data Protection Officer and Data Controllers/Champions, are committed to overseeing and upholding the compliance and adherence to this policy and all associated polices.

- LSEEG Group Executive Director Corporate Services (DPO)
- LSEC - Director MIS
- LSEC - Director HR
- LSEEG Group Director Marketing
- LSEC - Director IT
- LSEC - Technology Manager
- LSEC - Student Hub Manager/Admissions
- LSEEG Group Head Safeguarding
- LSEAT- Executive Head Teacher BBA/BTA
- LEAST – Executive Head Teacher New Horizons
- LSEAT – BBA/BTA – Head Teachers
- LSEAT – New Horizons Head of IT
- LSEAT – Business Manager BBA/BTA
- LSEAT – Business Managers New Horizons
- LSEAC – Director of Operations (LSECT)
- LSEAC – Recruitment Manager
- LSEAC – Director of Operations (LSfG)

APPENDIX C - RETENTION OF DATA & FREEDOM OF INFORMATION

RETENTION OF DATA

LSEEG will retain data as appropriate and lawful as defined in the Archive and documentation retention policy. Information about students cannot be kept indefinitely, unless there are specific requests to do so. In general information about students will be kept typically for a period of seven years after they leav LSEEG

All other information, including any information about health, race or disciplinary matters will not be routinely retained after one year of the course ending or the student leaving Bromley College, whichever is the sooner.

Bromley College will need to keep information about staff for longer periods of time. In general, all information will be kept for one year after a member of staff leaves Bromley College. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

FREEDOM OF INFORMATION REQUESTS FOR PERSONAL DATA

In some cases a Freedom of Information request (FOI) may refer to the requester's personal data. In this event such requests should be treated as a subject access request.

If it is not clear whether the request for personal data is made under the Freedom of Information Act, the College will process the request as a subject access request under this Policy.

APPENDIX D

STAFF GUIDELINES FOR GDPR

All staff will process data about students on a regular basis, when marking registers, or writing reports or references, or as part of a pastoral or academic supervisory role

LSEEG will ensure through registration procedures, that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the 1998 Act. The information that staff deal with on a day to day basis will be standard and will cover categories such as:

- General personal details such as name and address
- Details about class attendance, course work marks and grades and associated comments
- Notes of personal supervision, including matters about behaviour and discipline

Information about a student's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the students consent e.g. recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties. This is available from the Student Services team.

All staff have a duty to make sure that they comply with the data protection principles, which are set out in this GDPR Policy

Authorised staff will be responsible for ensuring that all data is kept securely.

Staff must not disclose personal data to any student, unless for normal academic or pastoral purposes, without express authorisation or agreement from the Data Protection Officer or Data Controller/Champion.

Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with Bromley College policy.

Before processing any personal data, all staff should consider the checklist.

STAFF CHECKLIST FOR RECORDING DATA

- Do you really need to record the information?
- Is the information standard or is it sensitive?
- If it is sensitive, do you have the data subject's express consent?
- Has the student been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?
- Have you reported the fact of data collection to the authorised person within the required time?

APPENDIX E
COMMITMENT TO TRAINING AND DEVELOPMENT

All staff will be trained and instructed appropriately based on their role. Training and instruction may be via:

- Formal induction training
- Training courses
- Leaflets, brochures
- The reading of policies and procedures
- SharePoint
- Instruction from managers or other staff
- Staff CPD programme
- External information (e.g. regulatory bodies, professional bodies)
- E-Learning

All employees have a responsibility to attend GDPR training when required and to sign attendance sheets or complete evaluations where appropriate.

Refresher training requirements must be arranged as appropriate. Where employed in a professional capacity staff must demonstrate ownership of their own CPD, for example though a CPD programme with their professional body.

Students will receive specific induction and training in GDPR as part of the curriculum and generally as required.