Group Data Protection and GDPR Policy

Responsible post holder	Group Chief Governance Officer & DPO
Approved by / on	Trust Board and College Corporation
Next Review	September 2028
Publication Method	Website

CONTENTS

A. STATEMENT OF INTENT

1. Introduction

The Statement of Intent sets our Group Management's commitment to data protection and describes the approach by which London South East Colleges, London South East Academies Trust and LASER Education Foundation and any subsidiary companies (the Group Organisations) meet their legal obligations.

2. Scope

The Group GDPR policy applies to all students, staff and contractors and covers all colleges and schools as well as activities off premises but under the individual organisation's control.

3. Policy Statement: Our Statement of Intent

London & South East Education Group, comprising London South East Colleges, London South East Academies Trust and LASER Education Foundation, the Group Organisations) has a mission and vision to transform lives through the power of learning.

We will strive to change people's lives, creating social value and promoting social mobility in every community we work with. We are enterprising in our approach, and as an agile, multifaceted education group, we enable and empower people of all ages from 5 to 95 to 'step up' to their next opportunity in life.

Education will always be at the core of our work but for our learners and community to thrive we recognise that qualifications alone are not enough. We want to build strong, sustainable communities that are economically and socially prosperous, and for our learners and partners to join us on this journey as co-producers in achieving this vision.

We recognise the importance of creating a fully compliant legal framework in which to discharge our legal responsibilities to protect and safeguard personal data and information, and to operate a model publication scheme as defined by the ICO.

We also recognise the role of our Group Organisations as a public funded bodies to provide appropriate training to our staff and students on data protection and requirement to safeguarding personal information an increasing digitised environment. To be open, lawful and transparent in the processing of personal information and data.

The leadership teams within our Group Organisations commit to:

- Take a sensible approach to data protection and balance the need to manage risks whilst delivering a great educational experience.
- Provide and maintain a safe environment for personal data held on all data subjects; staff, students, contractors, visitors and other people who involved with our activities.
- Formally defining the roles that all staff have in providing and maintaining data protection.

- Involve students and staff in through communication, consultation and direct involvement.
- Ensuring staff are trained and informed on all
- Take all reasonably practicable steps to eliminate, substitute or control risks within the workplace through risk identification, assessment, control and monitoring and review.
- Measure and communicate what works well and what needs improvement. This includes ensuring data breaches are reported, recorded and causes identified and ensure appropriate actions are taken to prevent reoccurrence.
- Continuously improve through regular review in line with the ICO guidance and direction.
- Be transparent, fair and lawful in the processing of personal data.
- Complying with all appropriate regulations and including;

    - ✓ Data Protection Act
    - ✓ Freedom of information
    - ✓ Subject Access Requests
    - ✓ DfE funding regulations and rules
    - ✓ Ofsted regulations and expectations
    - ✓ HMRC rules and regulations
    - ✓ Data regulations defined further by ICO
    - ✓ Regulations governing GFE, MATs and charities.

- Allocate resources to meet the commitments of this policy and review this policy annually.

B. ORGANISATIONS

London South East Colleges (LSEC)

The Statement of Intent sets out the LSEC's Management's commitment to GDPR and describes the approach by which the LSEC meets its data protection obligations.

1. Scope

The LSEEG GDPR policy applies to all paper and electronic information and covers all departments and areas, as well as activities off premises but under the LSEC's control.

2. Policy

Under the law the LSEEG has a number of legal duties. This documents how the LSEEG discharges those duties and specifies the responsibilities of key roles within the organisation. This policy should be read in conjunction with the Scheme of Delegation.

Role	Responsibility
LSEC Corporation	• Overall responsibility for the GDPR Policy • Agreeing the GDPR Policy Statement. • Approve the terms of reference of the LSEEG GDPR Committee. • To ensure that the LSEEG has suitable arrangements in place to make staff are aware of their data protection responsibilities and their need to comply with relevant data protection legislation.
Group CEO	• Executive responsibility for all GDPR matters and for ensuring the implementation of relevant LSEEG policy. • To ensure the LSEEG has in place the appropriate organisation and methods for the implementation of the GDPR Policy and for making all persons aware of their responsibilities. • To ensure that the correct emphasis is maintained on GDPR matters by all managers and ensure that correct standards of safe working are maintained for all staff and students and that appropriate resources are allocated to achieve this. • To ensure that Corporation are advised of the policy and that appropriate systems are in place to enable Corporation to supervise the LSEEG GDPR arrangements; to report to Corporation on an annual basis on the implementation of the GDPR Action Plan. • To set a personal example by following all rules and regulations when on site. • To have an understanding of the requirements laid down under the GDPR and data protection associated regulations, and any other statutory regulations, and ensure they are observed.
Group Data Protection Officer	• Corporate responsibility for GDPR is delegated to the Group DPO • Oversee the actions of the data protection and appropriate liaison with Directors, Delivery, Service and Support Team Managers.

	• To set in place and manage the organisation and method for implementing the GDPR Policy, and ensure that LSEEG Management, employees, students and contractors are aware of their responsibilities and the means of how they can be met.
	• To ensure the GDPR management systems, policies and amendments to them are disseminated through the LSEC to all relevant staff and other persons.
	• To have an understanding of the requirements laid down under the GDPR at GDPR, associated regulations, and any other statutory regulations, and ensure they are observed.
	• To ensure that policies are appropriately implemented by:
	  o Establishing monitoring and feedback arrangements
	  o Receiving formal reports regarding GDPR and acting on the information provided
	• To monitor LSEEG GDPR policies and procedures.
	• To set a personal example by following all rules and regulations when on site.
	• To Chair the LSEEG GDPR Committee.
	• To ensure that arrangements are in place for monitoring internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.
	• To ensure data controllers within the various areas of the organisation are competent and trained to monitor and safeguard data and supply sufficient support to allow accountability at all levels of the institution.
	• The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.
	• To report any serious incidents or occurrences to the LSEEG Board and CEO/Principal at the earliest opportunity.

Deputy CEO and Group CFO,	• Daily operational responsibility for GDPR is delegated through the Deputy CEO and CFO to Vice Principals, Career Pathway Director or Manages and Group or College Directors or Heads of Service
	• To manage the organisation and method for implementing the GDPR Policy, and ensure that LSEC Management, employees, students and contractors are aware of their responsibilities and the means of how they can be met.
	• To ensure the GDPR management systems, policies and amendments to them are disseminated through the LSEC to all relevant staff and other persons.
	• To have an understanding of the requirements laid down under the GDPR at data protection associated regulations, and any other statutory regulations, and ensure they are observed.
	• To ensure that policies are appropriately implemented by:
	  o Establishing monitoring and feedback arrangements
	  o Receiving formal reports regarding GDPR and acting on the information provided
	• To monitor LSEC GDPR policies and procedures.

	• To set a personal example by following all rules and regulations when on site. • To manage the data controller of the institution.
Data Controllers	• To have an understanding of the requirements laid down under the GDPR and data protection associated regulations, and any other statutory regulations, and ensure they are observed. • To ensure data impact assessments are completed where necessary to ensure data process are mapped and demonstrate how information is collected, stored, retrieved and removed. • To ensure arrangements are in place for annual GDPR assessments and review to be held at each LSEC Centre. • Deliver and/or arrange data protection training to staff to increase their knowledge and awareness and to fulfil statutory obligations as required. • To ensure employees receive training in GDPR matters as appropriate. • To ensure the LSEC receives appropriate external advice, guidance and support where required to implement the GDPR Policy.
COOs, Vice Principals Career Pathway Directors and Managers, Group or College Directors or Heads of Service	• Represent the LSEC leadership in terms of health and safety • Be initial point of contact in GDPR matters and data breach • Record events, investigate and communicate findings • Liaise with senior management and the DPO • Understand limits of competence and know when to escalate. • Ensure the effective planning, organisation, control, monitoring, review and auditing of the LSEC GDPR provision. • Submit GDPR reports and statistics where appropriate and where required. • Organise and manage the various levels of data processing and impact assessments. • Report on any matters which require their input in ensuring the effective GDPR of employees, learners, visitors and others.
Teachers and support staff	• Read and understand the LSEC's GDPR policy and supporting guidance documents to ensure that its provisions are being effectively carried out and maintained. • To have an understanding of the requirements laid down under the GDPR at data protection regulations and other appropriate regulations, and ensure they are observed. • Bring the provisions of this policy and the requirements of the GDPR to the attention of all employees and learners under their control. • Ensure all GDPR statutory documents and information electronic or paper are kept and stored securely and made available when required. • To ensure all employees in their areas receive mandatory GDPR training. • Always work within the frame work of GDPR and promote a positive culture and respect for data and information belonging to all data subjects. • To ensure that the updating, review and maintaining of GDPR related documents e.g. DPIAs are completed.

All staff	• Responsible for ensuring that they have a full understanding of GDPR and data protection. • Understand what to do in the event of a breach of data protection • Employees are responsible for adhering to the safeguarding of data as defined in the Statement of intent and the overarching data principles defined with the GDPR. • Take reasonable care around the safety and safekeeping of personal data. And understand that others may be affected by their acts or omissions. • Not to intentionally or recklessly interfere with or misuse anything provided in the interests of data protection in pursuance of any of the relevant statutory provisions. • Reporting of all data breaches within 24 hours of the breach or loss of data.
Behaviour, Safeguarding and Additional Learning Support Teams	• Student health and welfare teams - are to ensure that all data shared with third party agencies has received the additional authority to require from the data subject to authorised person or guardian representing the interest of the data subject. • Adhere to the GDPR policy and its associated links in relation to data sharing as defined in the Safeguarding Policy. • Understand the requirements under the GDPR policy to use the designated software to encrypt data when sharing with internal and external departments and organisations. • To restrict the sharing of information through email and use SharePoint and OneDrive to store and retain information in a safe and protected environment. • Up skill and develop other staff to participate effectively in data protection.

London South East Academies Trust

The Statement of Intent sets out the Trust's Management's commitment to GDPR and describes the approach by which the Trust meets its data protection obligations.

1. Scope

The Trust's GDPR policy applies to all paper and electronic information and covers all schools as well as activities off premises but under the Trust's control.

2. Policy

Under the law the Trust has a number of legal duties. This documents how the Trust discharges those duties and specifies the responsibilities of key roles within the organisation. This policy should be read in conjunction with the Scheme of Delegation.

Role	Responsibility
Trust Board	• Overall responsibility for the GDPR Policy • Agreeing the GDPR Policy Statement. • Approve the terms of reference of the Trust GDPR Committee. • To ensure that the Trust has suitable arrangements in place to make staff are aware of their data protection responsibilities and their need to comply with relevant data protection legislation.
Group CEO	• Executive responsibility for all GDPR matters and for ensuring the implementation of relevant Trust policy. • To ensure the Trust has in place the appropriate organisation and methods for the implementation of the GDPR Policy and for making all persons aware of their responsibilities. • To receive immediate verbal advice followed by written reports from the appropriate Manager on any fatality or serious occurrence out of or in connection with operations controlled by the Trust (including off-site collaborative provision and work placements) and to ensure that all statutory bodies are notified and relevant forms are completed. • To ensure that the correct emphasis is maintained on GDPR matters by all managers and ensure that correct standards of safe working are maintained for all staff and students and that appropriate resources are allocated to achieve this. • To ensure that Trustees are advised of the policy and that appropriate systems are in place to enable Trustees to supervise the Trust GDPR arrangements; to report to Trustees on an annual basis on the implementation of the GDPR Action Plan. • To set a personal example by following all rules and regulations when on site. • To have an understanding of the requirements laid down under the GDPR and data protection associated regulations, and any other statutory regulations, and ensure they are observed.
Group CFO	• Corporate responsibility for GDPR is delegated to the Deputy CEO

	• Oversee the actions of the data protection and appropriate liaison with Leadership and management and support team managers.
	• To set in place and manage the organisation and method for implementing the GDPR Policy, and ensure that Trust Management, employees, students and contractors are aware of their responsibilities and the means of how they can be met.
	• To ensure the GDPR management systems, policies and amendments to them are disseminated through the Trust to all relevant staff and other persons.
	• To have an understanding of the requirements laid down under the GDPR at GDPR, associated regulations, and any other statutory regulations, and ensure they are observed.
	• To ensure that policies are appropriately implemented by:
	  o Establishing monitoring and feedback arrangements
	  o Receiving formal reports regarding GDPR and acting on the information provided
	• To monitor Trust GDPR policies and procedures.
	• To set a personal example by following all rules and regulations when on site.

Group Data Protection Officer	• To Chair the GDPR Committee. • To ensure that arrangements are in place for monitoring internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority. • To ensure data controllers within the various areas of the organisation are competent and trained to monitor and safeguard data and supply sufficient support to allow accountability at all levels of the institution. • The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level. • To report any serious incidents or occurrences to the CEO and Trust Board al at the earliest opportunity.

Deputy CEO	• Daily operational responsibility for GDPR is delegated through the scheme of delegation to the Deputy CEO.
	• To manage the organisation and method for implementing the GDPR Policy, and ensure that Trust Management, employees, students and contractors are aware of their responsibilities and the means of how they can be met.
	• To ensure the GDPR management systems, policies and amendments to them are disseminated through the Trust to all relevant staff and other persons.
	• To have an understanding of the requirements laid down under the GDPR at data protection associated regulations, and any other statutory regulations, and ensure they are observed.
	• To ensure that policies are appropriately implemented by:
	  o Establishing monitoring and feedback arrangements
	  o Receiving formal reports regarding GDPR and acting on the information provided
	• To monitor Trust GDPR policies and procedures.

	• To set a personal example by following all rules and regulations when on site. • To manage the data controller of the institution.
Data Controllers (Group Service Directors)	• To have an understanding of the requirements laid down under the GDPR and data protection associated regulations, and any other statutory regulations, and ensure they are observed. • To ensure data impact assessments are completed where necessary to ensure data process are mapped and demonstrate how information is collected, stored, retrieved and removed. • To ensure arrangements are in place for annual GDPR assessments and review to be held at each Trust Centre. • Deliver and/or arrange data protection training to staff to increase their knowledge and awareness and to fulfil statutory obligations as required. • To ensure employees receive training in GDPR matters as appropriate. • To ensure the Trust receives appropriate external advice, guidance and support where required to implement the GDPR Policy.
Heads Teachers and Heads of School or delegates	• Represent the trust leadership in terms of health and safety • Be initial point of contact in GDPR matters and data breach • Record events, investigate and communicate findings • Liaise with senior management and the DPO • Understand limits of competence and know when to escalate. • Ensure the effective planning, organisation, control, monitoring, review and auditing of the trust GDPR provision. • Submit GDPR reports and statistics where appropriate and where required. • Organise and manage the various levels of data processing and impact assessments. • Report on any matters which require their input in ensuring the effective GDPR of employees, learners, visitors and others.
Teachers and support staff	• Read and understand the trust's GDPR policy and supporting guidance documents to ensure that its provisions are being effectively carried out and maintained. • To have an understanding of the requirements laid down under the GDPR at data protection regulations and other appropriate regulations, and ensure they are observed. • Bring the provisions of this policy and the requirements of the GDPR to the attention of all employees and learners under their control. • Ensure all GDPR statutory documents and information electronic or paper are kept and stored securely and made available when required. • To ensure all employees in their areas receive mandatory GDPR training. • Always work within the frame work of GDPR and promote a positive culture and respect for data and information belonging to all data subjects. • To ensure that the updating, review and maintaining of GDPR related documents e.g. DPIAs are completed.

All staff	• Responsible for ensuring that they have a full understanding of GDPR and data protection. • Understand what to do in the event of a breach of data protection • Employees are responsible for adhering to the safeguarding of data as defined in the Statement of intent and the overarching data principles defined with the GDPR. • Take reasonable care around the safety and safekeeping of personal data. And understand that others may be affected by their acts or omissions. • Not to intentionally or recklessly interfere with or misuse anything provided in the interests of data protection in pursuance of any of the relevant statutory provisions. • Reporting of all data breaches within 24 hours of the breach or loss of data.
Behaviour and Safeguarding Team	• Student health and welfare teams - are to ensure that all data shared with third party agencies has received the additional authority to require from the data subject to authorised person or guardian representing the interest of the data subject. • Adhere to the GDPR policy and its associated links in relation to data sharing as defined in the Safeguarding Policy. • Understand the requirements under the GDPR policy to use the designated software to encrypt data when sharing with internal and external departments and organisations. • To restrict the sharing of information through email and use SharePoint and OneDrive to store and retain information in a safe and protected environment. • Up skill and develop other staff to participate effectively in data protection.

C. Summary of Arrangement

1. Introduction

London & South East Education Group (LSEEG) has a number of arrangements in place to manage UK GDPR risks. This policy provides a summary of those arrangements.

2. Scope

The scope of these protocols and procedures covers all organisations currently within the LSEEG Group, which comprises London South East Colleges, London South East Academies Trust and LASER Education Foundation ("the Group Organisations").

3. Policy Accountabilities

3.1 The Principles of UK 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. The 9ine platfrom is used as a tool to assess and identify risks with regard to DPIAs.

We will appoint Data Controllers/Champions within the LSEEG Group and also within the Group Organisations themselves

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 Group Organisations.

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 Group 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 pseudonymisation 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 2018 (as amended) 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 UK GDPR policy and associated policies, have been prepared taking account of prevailing legislation and legislation requirements and follows best practice by enabling the Group Organisations 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 UK 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 the Group Organisations 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 the Group Organisations. 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

UK 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.

UK GDPR requires the Group Organisations 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 the Group Organisations operations will be covered where data and information is being processed, shared, retained or removed.

DPIAs will be standardised where possible 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 LSEEG Group.

DPIAs will be produced where the environment or activity varies greatly, for example Staff Recruitment Fairs, Marketing Roadshows, etc.

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 LSEEG 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.

9. Data Sharing

A Data and Information Sharing Policy has been developed by the College and the Trust (the Group Organisations) to facilitate the secure sharing of all personal, sensitive and non-personal information between the Group Organisations.

The LSEEG Data and Information Sharing Policy sets out the general principles, standards and governance agreed between the identified Group Organisation to provide a secure framework for the sharing of information within which they can all operate . It sets out the rules that all people working for or with the Group Organisations must follow when using and sharing information.

The LSEEG Data and Information Sharing Policy has been endorsed by the Governing Bodies of the Group Organisations with an undertaking to implement and adhere to key principles, at the heart of the general data protection regime set out in Article 5 of the UK General Data Protection Regulation (UK UK GDPR). Thus providing assurance to each that data and information will be processed used and managed only in agreed and appropriate ways as determined by the consent of the data subject and in accordance with each Group Organisations' Privacy Statements and conditional upon the information that is already shared for regulatory purposes with the Department for Education, ESFA, Local Authorities, Social Service and police authorities, as required.

A copy of the Group Data and Information Sharing Policy is available on the Group Organisations' individual websites.

10 Data Deletion – Right to Removal

A data subject can request to have their date deleted and removed. As a publicly funded body, it may be necessary to retain individual persona data for audit purposes. Details of how long information is held is referenced in 4.4 above. A request for data deletion request form is available on the website.

11. Use of AI, EdTech & Cloud Services

The Group recognises the growing use of artificial intelligence (AI), educational technology (EdTech), and cloud-based services in delivering education. All such tools must comply with the UK GDPR and the Data Protection Act 2018. Data Processing Agreements will be established with providers, risk assessments carried out for international transfers, and clear governance maintained to ensure safeguarding and data privacy. Staff must not input personal or sensitive student data into AI systems unless formally authorised by the Data Protection Officer.

APPENDIX A

SUBJECT ACCESS REQUEST PROCEDURE

INTRODUCTION

The Group Organisations are 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, the Group Organisations must comply with the UK GDPR Principles as defined above,

All the Group Organisations' 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, the Group Organisations have developed a Group UK GDPR Policy of which this procedure form's part.

The Group Organisations are 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 the Group Organisations hold 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 the Group Organisations are doing to comply with its obligations under UK GDPR.

The Group Organisations will provide all staff with a standard form of notification or privacy statement

This will state the types of data the Group Organisations hold 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 the Group Organisations in connection with their employment is accurate and up to date.
- Inform the Group Organisations they are employed 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 that the Group Organisations may send out from time to time,
- Inform the Group Organisations 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).

RIGHTS TO ACCESS INFORMATION

Staff, students and other users of the Group Organisations 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 the Group Organisations.

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.

The Group Organisations 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. In some instances it may be necessary to "stop the clock" to review and assess the information and data to be shared.

SUBJECT CONSENT

Where the Group Organisations have 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 the Group Organisations 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. The Group Organisations 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.

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

The Group Organisations 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. The Group Organisations 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 the Group Organisations are a safe place for everyone, or to operate other associated Group, Trust or College policies, such as the Managing Sickness Absence Policy.

The Group Organisations 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 the Group Organisation 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 Group Organisations' websites.

Subject Access Forms for the Group Organisations are available on the induvial websites.

Appendix B : Privacy Statements

London South East Academies Trust
Data Protection Privacy Statement : Students/Pupils

Contents

1. Introduction

1.1 Under data protection law, individuals have a right to be informed about how the Trust and its
Trust Schools use any personal data that is held about them. We, London South East Academies Trust, comply with this right by providing Privacy Notices to individuals where we are processing their personal data.

2. Document purpose

2.1 The purpose of this Privacy Notice is to explain how we, London South East Academies Trust and our Academies, collect, store and use personal data about your child/ward.

3. Data controller and processors

3.1 The Trust is the Data Controller for the purposes of data protection law and therefore will
determine the purposes for which personal data is processed (the 'why' and the 'how'). Our Academies and authorised 3rd parties, e.g. ParentPay, process and 'use' data on behalf of (under the supervision/control) the Trust and are therefore Data Processors.

3.2 The postal address for London South East Academy Trust is
London South East Academy Trust
Rookery Lane, Bromley BR2 8HE

3.3 The Trusts Data Protection Officer is Jennifer Pharo and her contact details are at Section 17

3.4 The Trust and its Academies will ensure that your child/ward's personal data is processed fairly and lawfully, is accurate, is kept secure and is retained for no longer than is necessary.

4. The categories of personal data we hold

4.1 We process data about the student/pupils who attend our Trust Schools.
Personal data that we may collect, use, store and share (when appropriate) about your child/ward includes, but is not restricted to:

- Personal information, including name, unique student/pupil number, address and contact details of parents/carers.
- Characteristics, such as ethnicity, language, nationality, country of birth and religion.
- Attendance information, such as sessions attended, number of absences and absence reasons.
- Information from social services, such as safeguarding information or care status.
- Test results, including National Curriculum assessment results (external) and Academy examination results (internal).
- Special educational needs information and free school meal eligibility.
- Any relevant medical conditions, including physical and mental health or any disabilities a student/pupil may have.
- Details of any behaviour issues or exclusion information.
- Details of any support received, including care packages, plans and support providers.
- Destinations of where your child/ward intends moving on to once they've left the Academy.
- Other, including Photographs, CCTV images captured in Trust Schools, Biometric data (in certain Trust Schools).

5. Why we use this data

5.1 We use this data to:

- Support student/pupil learning.
- Protect student/pupil welfare.
- Monitor and report on student/pupil progress.
- Provide appropriate pastoral care.
- Assess the quality of our services.
- Administer admissions waiting lists.
- Carry out education related research.
- Prevent and detect crime.
- Provide references for employment.

6. Our lawful basis for using this data

6.1 We will only collect and use your child/ward's personal data when the law allows us to. Most commonly, we will process it where:

- We need to comply with a legal obligation.
- We need to perform an official task in the public interest (i.e. in order to provide child/ward with an education).

6.2 Less commonly we may also use your child/ward's personal data where:

- We have obtained consent to use it in a certain way.
- We need to protect the individual's health interests (or someone else's interest).

6.3 Where we have obtained consent to use child/ward's data, this consent can be withdrawn at any time.
We will make this clear when we ask for consent and explain how consent can be withdrawn.

6.4 Some of the reasons listed above for collecting and using your child/ward's personal data overlap, and there may be several grounds which justify our use of this data.

7. Collecting this information

7.1 While the majority of information we collect about your child/ward is mandatory, there is some information that can be provided voluntarily. Whenever we seek to collect information from you or your child/ward, we will make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

7.2 We may also receive information from previous schools, the Local Authority(s) and/or the Department for Education (DfE). For children/wards enrolling post 14 years of age, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about your child/ward's learning qualification.

8. How we store this data

8.1 We keep personal information about your child/ward while they are attending one of our Trust Schools.

We will also keep it beyond their attendance at one of our Trust Schools if this is necessary in order to comply with our legal obligations.

8.2 We have a Records Retention Policy, which sets out how long we must keep information about your child/ward. You can request a copy from your Academy if you want to understand the timelines in more detail.

8.3

9. Data sharing

9.1 We do not share personal information about your child/ward with any third party without consent unless the law and our policies allow us to do so.

9.2 London South East Colleges is the Sponsor Organisation for London South East Academies Trust, as a result of this relationship and association, a **Data Sharing Policy** has been approved by the respective Governing Boards of both legal entities, to ensure and provide assurance that practice and procedures (where there is a legitimate requirement to share information between the two organisations), is with due consideration and regard for data protection law. For students/pupils this may be with regard to sharing individual information at the key points in a student/pupil progression and transition period from School to College.

A copy of this policy is available on the Trust website.

9.3 Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about your child/ward with:

- The Local Authority - to meet our legal obligations to share certain information with it, such as concerns about student/pupil's safety and exclusions.
- The Department for Education (a government department) - to meet our legal obligations as part of data collections such as the School Census (more detail below).
- Your family or representatives - in case of emergencies such as a health matter.
- Follow on schools - which a student/pupil attends after leaving their current Academy in the public interest of delivering education.
- Youth Support Services - as it has legal responsibilities regarding the education or training of 13-19-year-olds.
- Educators and examining bodies - necessary for the performance of our education function.
- Our regulator, Ofsted - to enable it to evaluate the education we provide to your child/ward, which is in the public interest.

- Suppliers and service providers - to enable them to provide the service we have contracted them for.
- Health and social welfare organisations / third parties - to enable us to comply with our duty of care and statutory safeguarding duties for your child/ward's wellbeing, including:
  - Therapists, clinical psychologists.
  - Academy medical staff / nurse.
  - School counsellors.
  - CAMHS (Child and Adolescent Mental Health Service).
  - Social care.
  - Educational Welfare Officer (EWO).
  - Police forces, courts, tribunals - to uphold law and order.

10. Department for Education

10.1 We are required to provide information about your child/ward to the Department for Education (a government department) as part of data collections, such as the school census.
To find out more about the student/pupil information we are required to share with the department, for the purpose of data collection, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools or National Pupil Database.

10.2 Some of this information is then stored in the National Pupil Database, which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research. The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

10.3 The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

10.4 You can find more information about this on the Department for Education's webpage on how it collects and shares research data. https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

10.5 You can also contact the Department for Education online via https://www.gov.uk/contact-dfe if you have any questions about the database.

11. Youth support services

11.1 Once your child/ward reaches the age of 13, we are legally required to pass on certain information about them to the local authority or youth support services provider in your area, as it has legal responsibilities regarding the education or training of 13-19 year-olds.

11.2 This information enables it to provide Youth Support Services, post-16 education and training services, and careers advice.

11.3 Parents/carers, or children once aged 16 or over, can contact their Academy Data Champion to ask to request that we only pass the student/pupil's name, address and date of birth to your local authority or Youth Support Services provider.

12. Transferring data internationally

12.1 Where we share data with an organisation that is based outside the European Economic Area, we will do so in accordance with data protection law.

12.2 This would only happen if one of the student/pupil's parents/carers lives abroad or if the child/ward intends moving to a new school abroad. If this happens, we will be very careful to make sure that it is safe to transfer any student/pupil information. We will look

at whether that other country has good data protection laws for example. If we cannot be sure that it is safe then we will talk to you, the child/ward's parent/carer, and make sure you are content for that information to be sent.

13. Photographs and media

13.1 As part of our Academy activities, we may take photographs and allow external organisations to take photographs or to film within our Trust Schools in line with our Photograph and Media Policy. Your child/ward will be made aware when this is happening and the context in which the photograph will be used.

13.2 An Academy will take photographs for its own use. Usually these will be unnamed and will generally be for internal Academy use, but may also include photographs for publication, such as:

- Photographs included in an Academy prospectus.
- Photographs to show as slides at an event for parents/carers.
- Photographs to be used on display boards, which can be seen by visitors to the school.
- Photographs posted on Academy official websites such as Twitter and Facebook sites.

Such sites can be accessed by the public and will therefore require close monitoring by Academy staff to ensure they are appropriate.

13.3 Named photographs will be used for internal use where there is a clear lawful basis for doing so e.g. for identification purposes such as a student/pupil, staff or visitor security pass, safeguarding requirements and as part of exclusion behaviour data.

13.4 For all other purposes, if an Academy wants to use named photographs then it will obtain specific parent/carer or student/pupil consent first. For student/pupils/pupils at Primary Trust Schools consent will be sought from parents/carers and at Secondary/Sixth Form Trust Schools this will most likely be student/pupil consent. However, when student/pupil consent is sought then the parental wishes will be taken into account wherever possible.

14. CCTV

14.1 Trust Schools operate CCTV on their premises. This is considered necessary to protect staff and student/pupil's safety and Trust property.

15. Parent, carer and student/pupil's rights

15.1 Individuals have a right to make a Subject Access Request to gain access to the personal information that we hold about them.

15.2 Parents/carers can make a request with respect to their child, young person or ward's data where the child, young person or ward is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child/ward has provided consent for this. In this regard we may request permission from a young person over the age of 13 to share personal data and information with their parent/carer. Where this may involve sensitive data including safeguarding, information this information may not be shared.

15.3 Parents/carers also have the right to make a Subject Access Request with respect to any personal data the Academy holds about them.

15.4 If you make a Subject Access Request, and if we do hold information about you or your child, we will:

- Give you a description of it.
- Tell you why we are holding and processing it, and how long we will keep it for.
- Explain where we got it from, if not from you or your child.
- Tell you who it has been, or will be, shared with.

- Let you know whether any automated decision-making is being applied to the data, and any consequences of this.
- Give you a copy of the information in an intelligible form
- Provide the information to you within one month of being made aware of the Subject Access Request.

Subject Access Request Forms are available on the Trust website.

15.5 If you want to make a request please contact your Academy Data Champion in the first instance or ask your child/ward's tutor if you are unsure who this is. Other rights

15.6 Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress.
- Prevent it being used to send direct marketing.
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person).
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing.

15.7 To exercise any of these rights, please contact your Trust School Data Champion in the first instance or the Trust Data Protection Officer (contact details below).

16. Complaints

16.1 We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

16.2 To make a complaint please contact our Data Protection Officer.

16.3 Alternatively, you can make a complaint to the Information Commissioner's Office in one of the following ways:

- Report a concern online at https://ico.org.uk/concerns.
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

17. Contact details

17.1 If you have any questions, concerns or would like more information about anything mentioned in this Privacy Notice, please contact your Data Champion in the first instance or the Trust's Data Protection Officer, details below: Jennifer Pharo at GDPR@lsec.ac.uk

---

London South East Colleges
Data Protection Privacy Statement : Students

Contents

1. Introduction

1.1 Under data protection law, individuals have a right to be informed about how the London South East Colleges (LSEC) uses any personal data that is held about them. We, London South East Colleges) , comply with this right by providing this Privacy Notices to individuals where we are processing their personal data.

2. Document purpose

2.1 The purpose of this Privacy Notice is to explain how we, the London South East Colleges (LSEC) , collect, store and use personal data about students.

3. Data controller and processors

3.1 London South East Colleges (LSEC) is the Data Controller for the purposes of data protection law and therefore will determine the purposes for which personal data is processed (the 'why' and the 'how').
Authorised 3rd parties, e.g. DfE, Awarding bodies, etc. process and 'use' data on behalf of (under the supervision/control) the London South East Colleges (LSEC) and are therefore Data Processors.

3.2 The postal address for London South East Colleges (LSEC) is
Rookery Lane
Bromley BR2 8HE

3.3 Group Data Protection Officer is Jennifer Pharo and her contact details are at Section 17.

3.4 London South East Colleges (LSEC)) and its various campuses will ensure that your personal data is processed fairly and lawfully, is accurate, is kept secure and is retained for no longer than is necessary.

4. The categories of personal data we hold

4.1 Students

We process data about the students who apply, enrol and attend all our courses and provision.
Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Personal information, including name, unique student number, address and contact details of parents/carers.
- Characteristics, such as ethnicity, language, nationality, country of birth and religion.
- Attendance information, such as sessions attended, number of absences and absence reasons.

- Information from social services, such as safeguarding information or care status.
- Test results and assessments – internal and external.
- Special educational needs information and free school meal eligibility.
- Any relevant medical conditions, including physical and mental health or any disabilities a student may have.
- Benefits, Immigration and home office information related to your eligibility to receive funding and participate in learning.
- Details of any behaviour issues or exclusion information.
- Details of any support received, including care packages, plans and support providers.
- Destinations of where you intend to progress or move on to once you have left LSEC.
- Other, including Photographs, Videos, CCTV images captured in London South East Colleges (LSEC) Sites.

5. Why we use this data

5.1 Students: we use this data to:

- Support student learning.
- Protect student welfare.
- Monitor and report on student progress.
- Provide appropriate pastoral care.
- Assess the quality of our services.
- Administer admissions waiting lists.
- Carry out education related research.
- Prevent and detect crime.
- Provide references for employment.

6. Our lawful basis for using this data

6.1 We will only collect and use your personal data when the law allows us to.
Most commonly, we will process it where:

- We need to comply with a legal obligation.
- We need to perform an official task in the public interest (i.e. in order to provide you with an education).

6.2 Less commonly we may also use your personal data where:

- We have obtained consent to use it in a certain way.
- We need to protect the individual's health interests (or someone else's interest).

6.3 Where we have obtained consent to use your data, this consent can be withdrawn at any time.
We will make this clear when we ask for consent and explain how consent can be withdrawn.

6.4 Some of the reasons listed above for collecting and using your child/ward's personal data overlap, and there may be several grounds which justify our use of this data.

7. Collecting this information

7.1 While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily. Whenever we seek to collect information from you, we will make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

7.2 We may also receive information from previous schools, the Local Authority(s) and/or the Department for Education (DfE). For students enrolling post 14 years of age, the

Learning Records Service will give us the unique learner number (ULN) and may also give us details about your learning qualification.

8. How we store this data

8.1 We keep personal information about you while you are attending London South East College (LSEC)) .
We will also keep it beyond your attendance at one of our organisations as this is necessary in order to comply with our legal obligations as a public institute receiving public funding.

8.2 We have a Records Retention Policy, which sets out how long we must keep information about you. You can request a copy of the by emailing GDPR@lsec.ac.uk if you want to understand the timelines in more detail.

9. Data sharing

9.1 We do not share personal information about you with any third party without consent unless the law and our policies allow us to do so.

9.2 London South East Colleges is the Sponsor Organisation for London South East Academies Trust, as a result of this relationship and association, a **Data Sharing Policy** has been approved by the respective Governing Boards of both legal entities, to ensure and provide assurance that practice and procedures (where there is a legitimate requirement to share information between the two organisations), is with due consideration and regard for data protection law. For students/pupils this may be with regard to sharing individual information at the key points in a student/pupil progression and transition period from School to College.

9.2 Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- The Local Authority - to meet our legal obligations to share certain information with it, such as concerns about student's safety and exclusions.
- The Department for Education (a government department) - to meet our legal obligations as part of data collections such as the ILR funding submission (more detail below).
- Your family or representatives - in case of emergencies such as a health matter.
- Follow on schools - which a student attends after leaving their current Academy in the public interest of delivering education.
- Youth Support Services - as it has legal responsibilities regarding the education or training of 13-19-year-olds.
- Educators and examining bodies - necessary for the performance of our education function.
- Our regulator, Ofsted - to enable it to evaluate the education we provide to your child/ward, which is in the public interest.
- Suppliers and service providers - to enable them to provide the service we have contracted them for.
- Health and social welfare organisations / third parties - to enable us to comply with our duty of care and statutory safeguarding duties for your child/ward's wellbeing, including:
    - Therapists, clinical psychologists.
    - Academy medical staff / nurse.
    - School counsellors.
    - CAMHS (Child and Adolescent Mental Health Service).
    - Social care.
    - Educational Welfare Officer (EWO).

- Police forces, courts, tribunals - to uphold law and order.

10. Department for Education

10.1 We are required to provide information about you to the Department for Education (a government department) as part of data collections, such as our monthly funding and data submission.

10.2 Some of this information is then stored and managed by the Department for Education and provides evidence on how colleges are funded and performing. This, in turn, supports research. The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from all college and providers, local authorities, exam boards and others.

10.3 The Department for Education may share information from the database with other organisations which promote education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

10.4 You can find more information about this on the Department for Education's webpage on how it collects and shares research data. https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

10.5 You can also contact the Department for Education online via https://www.gov.uk/contact-dfe if you have any questions about the database.

11. Youth support services – post 16 education

11.1 Wee are legally required to pass on certain information about you if you are aged between 16-18 or 19-24 with special educational needs, to the local authority or youth support services provider in your area, as it has legal responsibilities regarding you education or training

11.2 This information enables it to provide Youth Support Services, post-16 education and training services, and careers advice.

12. Transferring data internationally

12.1 Where we share data with an organisation that is based outside the European Economic Area, we will do so in accordance with data protection law.

12.2 This would only happen if you are under the age of 18 and have a parent or guardian who lives abroad. If this happens we will be very careful to make sure that it is safe to transfer any student information.

13. Photographs and media

13.1 As part of our college activities, we may take photographs and allow external organisations to take photographs or to film within our London South East Colleges (LSEC)) sites in line with our Photograph and Media Policy. You will be made aware when this is happening and the context in which the photograph will be used.

13.2 LSEC and LSFG will take photographs for its own use. Usually these will be unnamed and will generally be for internal use, but may also include photographs for publication, such as:

- Photographs included in our prospectus.
- Photographs to show as slides at an event.
- Photographs to be used on display boards.
- Photographs posted on our official web and media sites such as Twitter and Facebook sites.

Such sites can be accessed by the public and will therefore require close monitoring by staff to ensure they are appropriate.

13.3 Named photographs will be used for internal use where there is a clear lawful basis for doing so e.g. for identification purposes such as a student, staff or visitor security pass, safeguarding requirements and as part of exclusion behaviour data.

13.4 For all other purposes, if we want to use named photographs then we will obtain specific consent.

14. CCTV

14.1 London South East Colleges (LSEC) operate CCTV on all our premises. This is considered necessary to protect staff and student's safety and London South East Colleges (LSEC) property.

15. Your rights

15.1 Individuals have a right to make a Subject Access Request to gain access to the personal information that we hold about them.

15.2 If you make a Subject Access Request, and if we do hold information about you or your child, we will:

- Give you a description of it.
- Tell you why we are holding and processing it, and how long we will keep it for.
- Explain where we got it from, if not from you or your child.
- Tell you who it has been, or will be, shared with.
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this.
- Give you a copy of the information in an intelligible form
- Provide the information to you within one month of being made aware of the Subject Access Request.

- Parents/carers can make a request with respect to their young person or ward's data where the young person or ward is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child/ward has provided consent for this. In this regard we may request permission from a young person over the age of 13 to share personal data and information with their parent/carer. Where this may involve sensitive data including safeguarding, information this information may not be shared.

15.3 If you want to make a request please contact complete the appropriate fomr on our website.

15.4 Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress.
- Prevent it being used to send direct marketing.
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person).
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing.

15.7 To exercise any of these rights, please contact London South East Colleges (LSEC) Data Protection Officer at GDPR@lsec.ac.uk

16. Complaints

16.1 We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

16.2 To make a complaint please contact our Group Data Protection Officer.

16.3 Alternatively, you can make a complaint to the Information Commissioner's Office in one of the following ways:

- Report a concern online at https://ico.org.uk/concerns.

- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

17. Contact details

17.1 If you have any questions, concerns or would like more information about anything mentioned in this Privacy Notice, please contact Group Data Protection Officer, Jennifer Pharo at GDPR@lsec.ac.uk

---

Data Protection: Staff Privacy Statement
Comprises employees, volunteers, temporary and third party agency workers and from London South East Colleges and London South East Academies Trust "the Group Organisations"

Contents

1. Introduction

1.1 Under data protection law, individuals have a right to be informed about how the London & South East Education Group uses any personal data that is held about them. We, London & South East Education Group, comply with this right by providing this Privacy Notices to individuals where we are processing their personal data.

2. Document purpose

2.1 The purpose of this Privacy Notice is to explain how we, London & South East Education Group and its associated organisations of London South East Colleges and London South East Academies Trust, collect, store and use personal data about you.

3. Data controller and processors

3.1 London South East Colleges and London South East Academies Trust (the Group Organisations) are the Data Controllers for the purposes of data protection law and therefore will determine the purposes for which personal data is processed (the 'why' and the 'how').

Authorised 3rd parties, e.g. DfE, Awarding bodies, etc. process and 'use' data on behalf of (under the supervision/control) the Group Organisations are therefore Data Processors.

3.2 The postal address for the Group Organisations is
Rookery Lane, Bromley, Kent BR2 8HE

3.3 London & South East Education Group, Group Data Protection Officer is Jennifer Pharo and her contact details are at Section 15.

3.4 London & South East Education Group and its associated organisations of London South East Colleges and South East Academies Trust located at various sites and campuses will ensure that your personal data is processed fairly and lawfully, is accurate, is kept secure and is retained for no longer than is necessary.

4. The categories of personal data we hold for staff

We process data about the staff employed on a permanent, temporary or contractual, voluntary and seconded basis across all our provision and areas of the Group Organisations.

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Employment matters (including obtaining references, probation period reports, appraisals, attendance, conduct, personal development, internal post applications, interviews, appointments and promotions, leave and sickness absence, grievance issues and complaints, including academic misconduct investigations and employee disciplinary actions)
- Maintenance of employee records, including your emergency contact details
- Compliance with employment visa requirements
- Administering employee payments and salaries (including pensions and other employee benefits)
- Providing employee support services (including the Employee Assistance Programme and our Occupational Health Service)
- Provision of access to University sites and facilities, and use of IT services, including the IT systems tools you require for your role.
- Training records and personal information collected if enrolled on a course at one of our Group Organisations.

5. Why we use this data

We use this date to:

- Information required by the Home Office and UKVI, in connection with visa requirements and immigration
- HMRC in matters relating to pay, benefits and taxation
- Responding to requests for information from government bodies and their authorised agents in line with current UK Higher Education legislation
- Monitoring Equal Opportunities, Equal Pay and the Gender Pay Gap at the University
- Ensuring the safety and security of employees
- Safeguarding and promoting the welfare and wellbeing of employees
- Responding to requests related to your rights under UK Data Protection Law
- As a public authority under the Freedom of Information Act (2000), responding where lawful to requests for information
- And as otherwise allowed in UK law

Additionally, as a public authority, and in the public interest, your personal information may be used to:

- Provide operational information and aggregate statistics to improve the organisations performance and services
- Conduct authorised research, surveys and analysis, which may involve third-party data processors
- Some information you give us for the above purposes, will be collected and processed on the basis of your explicit consent, e.g. Equal Opportunities information.
- In an emergency situation, contact details you have given to us will be used in relation to your or others' vital interests.

6. Our lawful basis for using this data

6.1 We will only collect and use your personal data when the law allows us to.
Most commonly, we will process it where:

- We need to comply with a legal obligation.
- We need to perform an official task in the public interest.

6.2 Less commonly we may also use your personal data where:

- We have obtained consent to use it in a certain way.
- We need to protect the individual's health interests (or someone else's interest).

6.3 Where we have obtained consent to use your data, this consent can be withdrawn at any time.
We will make this clear when we ask for consent and explain how consent can be withdrawn.

6.4 Some of the reasons listed above for collecting and using your personal data overlap, and there may be several grounds which justify our use of this data.

7. Collecting this information

7.1 While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily. Whenever we seek to collect information from you, we will make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

8. How we store and retain this data

8.1 We keep personal information about you while you are employed or volunteer on any basis for our Group Organisations.

8.2 We have a Records Retention Policy, which sets out how long we must keep information about you. You can request a copy of the by emailing GDPR@lsec.ac.uk or through the Group HR Department, if you want to understand the timelines in more detail.

9. Data sharing

9.1 We do not share personal information about you with any third party without consent unless the law and our Group Organisations' policies allow us to do so.

9.2 London South East Colleges is the Sponsor Organisation for London South East Academies Trust, as a result of this relationship and association, a **Group Data Sharing Policy** has been approved by the respective Governing Boards of both legal entities (the Group Organisations), to ensure and provide assurance that practice and procedures (where there is a legitimate requirement to share staff information between the two organisations), is with due consideration and regard for data protection law,

such data may relate to training, professional development, health & wellbeing and recruitment opportunities.

A copy of this policy is available on the Trust and College website.

9.3 Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- The Local Authority - to meet our legal obligations to share certain information with it.
- The Department for Education (a government department) - to meet our legal obligations as part of safeguarding legislation and workforce development.
- Your family or representatives - in case of emergencies such as a health matter.
- Educators and examining bodies - necessary for the performance of our education function.
- Suppliers and service providers - to enable them to provide the service we have contracted them for.
- HRMC, for payroll and pension related matters.
- Health and social welfare organisations / third parties - to enable us to comply with our duty of care and statutory safeguarding duties to you and our students.
    - Therapists, clinical psychologists.
    - Health and Safety/First Aiders
    - Occupational Health providers.
    - Police forces, courts, tribunals - to uphold law and order.
- Where necessary, we may receive personal data about you from third parties. Examples include the following:
    - Your previous employment record
    - Personal and contact details, your application and CV
    - Employment Agencies
    - Your immigration status
    - Home Office (UKVI)
    - Information about criminal convictions (where appropriate)
    - Disclosure & Barring Service
    - Medical, mental health, accessibility-related and similar information
    - (we only obtain this information from third parties if you give us consent to do so)
    - Medical practitioners/ occupational health.

10. Transferring data internationally

10.1 Where we share data with an organisation that is based outside the European Economic Area, we will do so in accordance with data protection law.

11. Photographs and media

11.1 As part of our business activities, the Group Organisations may take photographs and allow external organisations to take photographs or to film within our sites in line with our Photograph and Media Policy. You will be made aware when this is happening and the context in which the photograph will be used.

11.2 LSEC will take photographs for its own use. Usually these will be unnamed and will generally be for internal Academy use, but may also include photographs for publication, such as:

- Photographs included in prospectus.
- Photographs to show as slides at an event.
- Photographs to be used on display boards.

- Photographs posted on our official web and media sites such as Twitter and Facebook sites.

Such sites can be accessed by the public and will therefore require close monitoring by our staff to ensure they are appropriate.

11.3 Named photographs will be used for internal use where there is a clear lawful basis for doing so e.g. for identification purposes such as a student, staff or visitor security pass, safeguarding requirements and as part of exclusion behaviour data.

11.4 For all other purposes, if we want to use named photographs then it will obtain specific consent.

12. CCTV

12.1 The Group Organisations operate CCTV on all our premises. This is considered necessary to protect staff and student's safety and our property.

13. Your rights

13.1 Individuals have a right to make a Subject Access Request to gain access to the personal information that we hold about them.

13.2 If you make a Subject Access Request, and if we do hold information about you or your child, we will:

- Give you a description of it.
- Tell you why we are holding and processing it, and how long we will keep it for.
- Explain where we got it from, if not from you.
- Tell you who it has been, or will be, shared with.
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this.
- Give you a copy of the information in an intelligible form
- Provide the information to you within one month of being made aware of the Subject Access Request.

13.3 If you want to make a request, please contact complete the appropriate for on our website.

13.4 Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress.
- Prevent it being used to send direct marketing.
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person).
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing.

13.5 To exercise any of these rights, please contact the Group Data Protection Officer at GDPR@lsec.ac.uk

14. Complaints

14.1 We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

14.2 To make a complaint please contact our Group Data Protection Officer at GDPR@lsec.ac.uk

14.3 Alternatively, you can make a complaint to the Information Commissioner's Office in one of the following ways:

- Report a concern online at https://ico.org.uk/concerns.
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

15. Contact details

15.1 If you have any questions, concerns or would like more information about anything mentioned in this Privacy Notice, please contact the Group Data Protection Officer, Jennifer Pharo at GDPR@lsec.ac.uk.

Privacy Notice for Governors and Trustees

1. Introduction

This privacy notice explains how we collect, store, and use personal data about individuals who serve as governors or trustees of LSEAT, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. The Personal Data We Hold

We may collect and process the following information:

- Name, address, contact details (email and phone)
- Date of birth
- EDI information
- Photographs
- Appointment details, role and responsibilities
- Criminal record checks (DBS certificates)
- Business and financial interests
- Attendance records
- Declaration of interests and meeting contributions
- Relevant qualifications and employment history
- Skill Audit
- Training and Development records

3. Why We Use This Data

We use this data to:

- Fulfil our statutory obligations as a maintained school or academy trust
- Facilitate effective governance and leadership
- Ensure safeguarding and suitability to work with children
- Communicate with governors/trustees and provide access to relevant systems
- Maintain statutory records (e.g. GIAS: Get Information About Schools)

4. Lawful Basis for Processing

We process this personal data under:

- Article 6(1)(c) – Legal obligation

- Article 6(1)(e) – Public task
- Article 9(2)(g) – Reasons of substantial public interest (for special category data)

5. Data Sharing.
We may share your information with:
- The Department for Education (DfE)
- Local Authorities
- Regulatory bodies such as Ofsted
- Companies providing governance systems (e.g., GovernorHub)
- The public, where legally required (e.g., business interests)
- Within our organisations

6. Data Retention
We keep personal data only as long as necessary to fulfill the purposes we collected it for. This is outlined in our Data Retention Policy, available upon request.

7. Your Rights
Under data protection law, you have rights including:
- Access to your personal data
- Correction of incorrect or incomplete data
- Request erasure (in limited circumstances)
- Objection to processing
- Request restriction of processing

8. Contact Us
If you have questions, or wish to exercise your rights, please contact:
- Data Protection Officer
- Jennifer Pharo
- jennifer.pharo@lsec.ac.uk
- Group Chief Governance Officer
- Rookery Lane, Bromley BR2 8HE

You also have the right to lodge a complaint with the Information Commissioner's Office (ICO) at www.ico.org.uk

APPENDIX C

DATA PROTECTION OFFICER AND THE DESIGNATED DATA CONTROLLERS/ CHAMPIONS

The following post holders, as designated roles of the Group Organisation provide assurance in the discharge of functions applicable under this policy, as the Group Data Protection Officer and Data Controllers/Champions, and who are committed to overseeing and upholding the compliance and adherence to this policy and all associated polices.

- Group Chief Governance Officer (DPO)
- Group Chief People Officer
- Group Director Safeguarding
- Group Director Marketing
- Group Director IT & Estates
- Group Director Finance
- Group Head Health & Safety
- Group Head of Operations & Estates
- LSEC Director Safeguarding
- LSEC Director Additional Learning Support
- LSEC Director MIS
- LSEC Director HR
- LSEC Director Quality
- LSEC Digital Transformation & Data Compliance Manager
- LSEC Technical Operations Manager
- LSEC Student Hub Manager/Admissions
- LSEC Head of Information Systems
- LSEAT- Head Teachers and Heads of School
- LSEAT Deputy & Assistant Head Teachers
- LSEAT School Business Managers
- LSEAT Office Managers
- LSEAT IT Service Providers
- MIS Managers and Staff
- HR Managers and Staff
- IT Managers and Staff
- Finance Managers and Staff
- Student Administration Managers and Staff
- School Office Managers and Staff.
- Safeguarding Managers and Staff across College and Trust.

APPENDIX D - RETENTION OF DATA & FREEDOM OF INFORMATION

RETENTION OF DATA

The Group Organisations 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 leave the Group Organisations.

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.

A Data Retention and Archive Policy for both the College and Trust are available upon request and cover all the statutory and regulatory periods for retaining pupils, students and staff data.

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 E

STAFF GUIDELINES FOR DATA PROTECTION (UK 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

The Group Organisations 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 UK 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 Group HR Policies.

Before processing any personal data whether student or staff related, 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 F

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
- AI
- Cybersecurity

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

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