GROUP DATA & INFORMATION SHARING POLICY

Responsible	Group Executive Director Governance and Group Data Protection Officer
Document Title & Reference	Group Data & Information Sharing Policy
Status	FINAL
Publication Date	July 2021
Review Date	July 2023
Approved/Ratified	LSEC AND LSEAT Boards

CONTENTS

1. Introduction and Preface ……..3
2. Scope 4
3. Aims and Objectives 5
4. The Legal Framework 5
5. Information covered by this Policy 6
6. Responsibilities when Sharing Information 7
7. Restrictions on use of Information Shared 8
8. Consent – Applies to Personal Data only 8
9. Indemnity 9
10. Security 9
11. Information Quality 10
12. Training 10
13. Individual Responsibilities 10
14. General Principles 10
15. Audit and Review Arrangements 111

Group Information Sharing Policy

This Policy applies to **London South East Colleges (LSEC**) a trading name of Bromley College of Further and Higher Education, a Further Education College incorporated under the Further and Higher Education Act 1992, of Rookery Lane, Bromley, Kent BR2 8HE (the **'College'**); and **London South East Academies Trust** a Multi Academy Trust**,** limited company and exempt charity (Company Registration Number: 09028122) **whose** registered office is Rookery Lane, Bromley Kent BR2 8HE ("LSEAT") (the '**Trust**').

For the purpose of this policy, both parties will be known as Group Organisations of London & South East Education Group (the '**Group Organisations'**).

Information and data that forms part of this sharing policy will be covered by a **Group Organisation Data Processing Agreement,** which will underpin this policy and provide the legal basis for the processing of data and information that is shared between the two organisations.

1. Introduction and Preface

This Data and Information Sharing Policy has been developed by the College and the Trust to facilitate the secure sharing of all personal, sensitive and non-personal information between London & South East Education Group Organisations.

For the purpose of this Policy, the terms data and information are synonymous.

This 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.

By endorsing and approving this policy, the Group Organisations undertake to implement and adhere to the principles, standards and governance set out in this Policy reassuring the each organisation 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.

This Policy will be underpinned by seven key principles which lie at the heart of the general data protection regime set out in Article 5 of the UK General Data Protection Regulation (UK GDPR) which requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

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

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

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').between the parties and ensures that this is designed to meet the specific requirements for the sharing of specific information for specific purposes using specific systems.

1.1 The parties to this Policy provide educational services to the public and have a legal responsibility to ensure that their use of personal data is lawful, properly controlled and that an individual's rights are respected. This balance between the need to share personal data to provide quality service and protection of confidentiality is often a difficult one to achieve.

1.2 The legal situation regarding the protection and use of personal data can be unclear. This situation may lead to information not being readily available to those who have a genuine need to know in order for them to do their job properly.

1.3 There are fewer constraints on the sharing of non-personal data that is data which either does not identify a living individual or when combined with other information that is in or may come into the organisation's possession will not identify a living individual.

1.4 The parties to this Policy should ensure that all of their staff who are affected by it are:
- aware of its contents; and
- the obligations it and any information processing agreement (IPA) between the parties.

1.5 Each party/department should also ensure that revisions to the protocol and information sharing arrangements raised in it are endorsed and agreed in good time, which should be before any sharing takes place.

2. Scope

2.1 The overarching protocols of this Policy set out the principles for information sharing between the College and the Trust as Group Organisations.

2.2 This Policy will be further extended to include other public sector, working for or with the Group Organisations, to deliver services, for example social services, police.

2.3 This Policy sets out the rules that all people working for or with the Group Organisations must follow when using and sharing information.

2.4 This Policy applies to all information shared by Group Organisations. Sharing is **not** restricted solely to information classified as Personal Data by the Data Protection Act 2018 but may including the following:

a) All information processed by the Group Organisations including electronically (e.g. computer systems, CCTV, Audio etc.), or in manual records.

b) Anonymised, including aggregated data. The considerations, though less stringent, must take into account factors such as commercial or business, sensitive data, and the effect of many data sets being applied.

2.5 The specific purpose for use and sharing information will be defined in any other Information Policy that the College and or Trust enters into that will be specific to the Group Organisation sharing information.

3. Aims and Objectives

3.1 The aim of this protocol is to provide a framework for the Group Organisations and to establish and regulate working practices between Group Organisations. The protocol also provides guidance to ensure the secure transfer of information, and that information shared is for justifiable legal purposes (see 6.3 and 11.5).

3.2 These aims include:

a) To guide Group Organisation on how to share personal information lawfully and to identify the legal basis for information sharing.
b) To explain the security and confidentiality laws and principles of information sharing.
c) To increase awareness and understanding of the key issues.
d) To emphasise the need to develop and use this Information Sharing Policy.
e) To support a process that will monitor and review all information flows.
f) To encourage flows of information.
g) To protect the Group Organisation from accusations of wrongful use of personal data.

3.3 By endorsing this policy, the Group Organisations are making a commitment to:

a) Apply the Information Commissioner's Code of Practice's 'Fair Processing' and 'Best Practices' Standards.
b) Adhere to or demonstrate a commitment to achieving the appropriate compliance with the Data Protection Act 2018.
c) Endorse a Data Processing Agreement that specifies data processing procedures assigned to each other.

3.4 The Group Organisations are expected to promote staff awareness of the major requirements of Information Sharing and Processing. This will be supported by the production of appropriate guidelines and communications via intranets, training and induction, and access to the relevant encryption applications and software when sharing information between organisations.

3.5. The Group DPO convenes a Termly Steering Group of data controllers and processors with responsibilities across the Group Organisations, to facilitate and discuss best practice, identify common themes for training, development and process review.

4. The Legal Framework

4.1 The principal legislation concerning the protection and use of personal information is listed below and further explained in:

- Access to Health Records Act 1990
- Criminal Procedures and Investigations Act 1996
- Human Rights Act 1998 (article 8)
- Data Protection Act 2018

- UK General Data Protection Regulation (Regulation (EU) 2016/679 (United Kingdom General Data Protection Regulation (UK GDPR)
- Crime and Disorder Act 1998
- The Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Children Act 2004 and the Information Sharing Index
- Civil Contingencies Act 2004
- Computer Misuse Act
- The Common Law Duty of Confidence
- Equality Act 2010
- Care Act 2014

4.2 This is not an exhaustive list and other legislation may be relevant when sharing or processing specific information.

4.3 As part of this Information Sharing Policy, Group Organisations should identify how they will meet its legal obligations and the legal basis (legislation and appropriate section(s)) under which information may be shared and or processed.

5. Information Covered by this Policy

5.1 All Information, including personal data and sensitive personal data as defined in the Data Protection Act 2018 (DPA) and under UK GDPR Regulations. In order to reduce the risks of DPA compliance and security breaches, anonymised data should be used where possible.

5.2 Personal Data

The term 'personal data' refers to **any** data held as either manual or electronic records, or records held by means of audio and/or visual technology, about an individual who can be personally identified from that data. The term is further defined in the Data Protection Act 2018 (DPA) and UK General Data Protection Regulations (GDPR)

- Data relating to a living individual who can be identified from those data; or
- Any other information which is in the possession of or is likely to come into the possession of the data controller (person or organisation collecting that information).

The DPA also defines certain classes of personal information as 'sensitive data' where additional conditions must be met for that information to be used and disclosed lawfully.

An individual may consider certain information about them to be particularly private and may request other data items to be kept especially confidential e.g. any use of a pseudonym where their true identity needs to be withheld to protect them.

5.3 Anonymised Data

Organisation should ensure anonymised data, especially when combined with other information from different agencies, **does not** identify an individual, either directly or by summation.

Anonymised data about an individual can be shared without consent (subject to certain restrictions regarding health/social care records), in a form where the identity of the individual cannot be recognised i.e. when:

- Reference to any data item that could lead to an individual being identified has been removed.
- The data cannot be combined with any data sources held by a Partner to produce personal identifiable data.

6. Responsibilities when Sharing Information

6.1 General

Each Group Organisation is responsible for ensuring that their organisational and security measures protect the lawful use of information shared under this policy.

Group Organisations will ensure a reasonable level of security for supplied information, personal or non-personal, and process the information accordingly.

Group Organisations accept responsibility for independently or jointly auditing compliance with the Information Sharing Policy in which they are involved within reasonable timescales.

Every organisation should consider making it a condition of employment that employees will abide by their rules and policies in relation to the protection and use of confidential information. This condition should be written into employment contracts and any failure by an individual to follow the policy should be dealt with in accordance with that organisation's disciplinary procedures.

Every organisation should ensure that their contracts with external service providers include a condition that they abide by their rules and policies in relation to the protection and use of confidential information.

The Group Organisations originally supplying the information should be notified of any breach of confidentiality or incident involving a risk or breach of the security of information.

Group Organisations should have a written policy for retention and disposal of information.

Group Organisations must be aware that a data subject may withdraw consent to processing (i.e. Section 10 DPA 2018) of their personal information. In this case, processing can only continue where an applicable Data Protection Act Schedule 2, and if relevant Schedule 3, purpose applies.

Where the Group Organisation rely on consent as the condition for processing personal data then withdrawal means that the condition for processing will no longer apply. Withdrawal of consent should be communicated to Group Organisation and processing cease as soon as possible.

6.2 Personal Data

Personal data should only be shared for a specific lawful purpose or where appropriate consent has been obtained.

Staff should only be given access to personal data where there is a legal right, in order for them to perform their duties in connection with the services they are there to deliver.

This Policy does not give licence for unrestricted access to information another Group Organisation may hold. It sets out the parameters for the safe and secure sharing of

information for a justifiable **need to know** purpose.

Both parties to this Policy are responsible for ensuring every member of its staff is aware and complies with the obligation to protect confidentiality and a duty to disclose information only to those who have a right to see it.

Each party to the organisation should ensure that any of its staff accessing information under this Information Sharing Policy are trained and fully aware of their responsibilities to maintain the security and confidentiality of personal information.

Each organisation should ensure that any of its staff accessing information under an Information Sharing Policy to follow the procedures and standards that have been agreed and incorporated within this Information Sharing Policy.

Each Group Organisation will share information in compliance with the principles set out at Section 1 and in compliance with associated and relevant legislation set out in Section 4 and any other obligations detailed in the Policy.

Personal data shall not be transferred to a country or territory outside the EEA without an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

6.3 Non-Personal Data

Both organisations should not assume the non-personal information is not sensitive and can be freely shared. This may not be the case and the partner from whom the information originated from should be contacted before any further sharing takes place.

7. Restrictions on use of Information Shared

7.1 All shared information, personal or otherwise, must only be used for the purpose(s) specified at the time of disclosure(s) as defined in the relevant Information Sharing Policy unless obliged under statute or regulation, or under the instructions of a court or as agreed elsewhere. Therefore any further uses made of this data will not be lawful or covered by this Policy.

7.2 Restrictions may also apply to any further use of non-personal information, such as commercial sensitivity or prejudice to others caused by the information's release, and this should be considered when considering secondary use for non-personal information. If in doubt the information's original owner should be consulted.

7.3 Additional Statutory restrictions apply to the disclosure of certain information for example Criminal Records, HIV and AIDS, Assisted Conception and Abortion, Child Protection etc. Information about these will be included in any separate information sharing arrangements with third party organisations usually, Local Authorities, Social Services, Police and PHE.

8. Consent – Applies to Personal Data only

8.1 Consent is not the only means by which personal data can be disclosed. Under the Data Protection Act 2018 and UK General Data Protection Regulation in order to disclose personal data at least one condition in schedule two must be met. In order to disclose sensitive personal data at least one condition in both schedules two and three must be met.

8.2 Where a one of the parties has a statutory obligation to disclose personal data then the

consent of the data subject is not required; but the data subject should be informed that such an obligation exists.

8.3 If one of the organisations decides not to disclose some or all of the personal data, the requesting authority must be informed.

8.4 Consent has to be signified by some communication between the organisation and the Data Subject. If the Data Subject does not respond this cannot be assumed as implied consent. When using sensitive data, explicit consent must be obtained subject to any existing exemptions. In such cases the data subject's consent must be clear and cover items such as the specific details of processing, the data to be processed and the purpose for processing.

8.5 If consent is used as a form of justification for disclosure, the data subject must have the right to withdraw consent at any time.

8.6 Specific procedures will apply where the data subject is either not considered able to give informed consent itself because of either the data subject's age or where the data subject has a condition which means the data subject does not have the capacity to give informed consent. In these circumstances the relevant policy of the group should be referred to.

9. Indemnity

9.1 Each Group Organisation will keep each of the other partners fully indemnified against any and all costs, expenses and claims arising out of any breach of this Policy and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its sub-contractors, employees, agents or any other person within the control of the offending partner of any personal data obtained in connection with this Policy.

10. Security

10.1 It is assumed that each organisation will comply with the Group GDPR Statement of Intent and agree on security procedures. This should take account of the security classification of the information.

10.2 The Group Organisations agrees to adhere to the agreed standards of security. If there is a security breach in which information received from another party under this Information Sharing Policy is compromised, the originator will be notified at the earliest opportunity via the post holder identified at 3.2 of the ISA, who must forward details to the Information Security Section.

10.3 Where the Group Organisation has regular, specific security requirements, for example a corporate policy, either these or, if available, a hypertext link to the protocol should be included. This should help to avoid reviewing standards agreed previously when each new ISA is set up.

10.4 Security requirements will not be included in individual Information Sharing Policy except where they are unique to that Policy. This will ensure requirements are kept current, as notified, and avoid errors arising from having more than one copy of any third part organisations' standard requirements.

11. Information Quality

11.1 Information quality needs to be of a standard fit for the purpose information is to be used for, including being complete, accurate and as up to date as required for the purposes for which it is being shared. Without this any decision made on the information may be flawed and inappropriate actions may result. Group Organisation are expected to ensure that the Personal Data and Sensitive Personal Data that it holds is processed in accordance with DPA principles: this includes ensuring that the Data is accurate, complete and up-to-date and is not kept any longer than is necessary.

11.2 Where the Group Organisation share information under this Protocol it is expected that the Group Organisation will adopt ICO quality principles and Code of Practice and the supporting processes and procedures in place or be formally working towards this.

11.3 Group Organisations are expected to give undertakings that information meets a reasonable quality level for the proposed purposes for which it is being shared and be able to evidence this.

12. Training

12.1 All Group Organisation's employees processing information shared under this Policy are expected to be trained to a level that enables them to undertake their duties confidently, efficiently and lawfully. This is a legal obligation of each Group Organisation and responsibility for it cannot be assigned to another organisation, although delivery of training can be assigned.

12.2 To minimise the costs associated with training and to ensure that all staff participating in activities based on information shared under this Policy the College and Trust have access to online resources and guidance on training materials, accessed via the intranet and through College and Trust wide communications.

13. Individual Responsibilities

13.1 Every individual working for the Group Organisations listed in this Policy is personally responsible for the safekeeping of any information they obtain, handle, use and disclose.

13.2 Every individual should know how to obtain, use and share information they legitimately need to do their job.

13.3 Every individual has an obligation to request proof of identity or takes steps to validate the authorisation of another before disclosing any information requested under this Policy.

13.4 Every individual should uphold the general principles of confidentiality, follow the guidelines of UK GDPR and seek advice when necessary.

13.5 Every individual should be aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could lead to their dismissal. Criminal proceedings might also be brought against that individual.

14. General Principles

14.1 The principles outlined in this Policy are recommended good standards of practice or legal requirements that should be adhered to by the Group Organisations.

14.2 This Policy sets the core standards applicable to the Group Organisations and should form the basis of all information sharing procedures established to secure the flow of personal information and adhere to the Information Processing Agreement between the parties.

14.3 This Policy should be used in conjunction with local service level Policy, contracts or any other formal Policy that exist between the Group Organisations.

14.4 All parties signed up to this Policy are responsible for ensuring that organisational measures are in place to protect the security and integrity of personal information and that their staff are properly trained to understand their responsibilities and comply with the law.

14.5 This Policy has been written to set out clear and consistent principles that satisfy the requirements of the law that all staff must follow when using and sharing personal information.

15. Audit and Review Arrangements

15.1 The Group Organisation accepts responsibility for independently or jointly auditing its own compliance with this Information Sharing Policy in which it is involved on a regular basis.

15.2 The Group Organisation is required to keep and maintain records of all requests for information sharing received and track the flow of Personal Confidential Data.

15.3 This overarching Policy will be formally reviewed periodically.

15.4 Either of the Group Organisations can request an extraordinary review at any time where a joint discussion or decision is necessary to address local service developments.