HUMAN RESOURCES POLICIES AND PROCEDURES	LEWISHAM SOUTHWARK COLLEGE
Policy title:	**Data Protection policy and procedure**
Applies to:	**All employees/contractors/students/visitors**
Owner of policy:	**Human Resources (HR) Department**

17. Impact assessment

Appendices:

Appendix 1: Guidelines for data protection
Appendix 2: Standard request form for access to data

1. Introduction and scope

1.1 The College keeps certain information about its employees, students and other users to allow it to monitor performance, achievement and health and safety. It is also necessary to process information so that employees can be recruited and paid, courses organised and to enable legal obligations to funding bodies and government to be complied with.

1.2 To comply with the law, information must be collected and used fairly, stored safely and not unlawfully disclosed to any other person. To do this the College must comply with the data protection principles set out in the Data Protection Act 1998. In summary the data protection principles state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;
- Be obtained for a specified and lawful purpose and not be processed in any manner incompatible with that purpose;
- Be adequate, relevant and not excessive for those purposes;
- Be accurate and kept up to date;
- Not be kept for longer than is necessary for that purpose;
- Be processed in accordance with the data subject's rights;
- Be kept safe from unauthorised access, accidental loss or destruction;
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

1.3 The College and all employees 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 College has developed this Data Protection policy.

1.4 This policy applies to all employees as well as agency and casual employees and any contractors working at the College. It also applies to students and visitors to the College.

2. Policy objectives

2.1 This policy aims to:

- Raise awareness of the responsibilities and legal obligations for employees, when processing data;
- Clearly set out the rules regarding the processing of information.

3. Responsibilities: Managers

3.1 All managers are required to:

- draw to the attention of new employees their data protection responsibilities during induction;
- The College will provide training in Data Protection to all new employees.

4. Responsibilities: Employees

4.1 All employees are required to:

- Check that any information they provide to the College in connection with their employment is accurate and up to date;
- Inform the College of any changes to information, which they have provided e.g. changes of address, contact numbers, names etc.;
- Inform the College of any errors or changes.

4.2 The College cannot be held responsible for any errors unless the employee has informed the College of their up to date details.

4.3 If and when, as part of their responsibilities, employees collect information about other people, e.g. about students' course work, opinions, ability, references to other academic institutions, or details of personal circumstances, they must comply with the guidelines for employees, which are set out in Appendix 1.

4.4 All employees are responsible for ensuring that:

- Any personal data which they hold are kept securely;
- Personal information is not disclosed either orally, in writing or otherwise to any unauthorised third party;
- Accidental disclosure is avoided by ensuring that all procedures are appropriate and data are stored securely.

4.5 Any unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct where there is a safeguarding, equalities or health and safety implications.

4.6 Personal information should be:

- Kept in a locked filing cabinet or
- In a locked drawer; or
- If it is computerised, be password protected,, or
- Kept only on disc, which is itself kept securely.

4.7 This policy does not form part of the formal contract of employment. It is however a condition of employment that all employees will abide by the rules and policies made by the College. Any failure to follow the policy can therefore result in disciplinary proceedings.

4.8 Any employee who considers that the policy has not been followed in respect of personal data about themselves, should initially raise the matter with one of the College designated data controllers (see Section 12). If the matter is not resolved it should be raised as a formal grievance under the Grievance Policy.

5. Responsibilities: Students

5.1 All students are responsible for:

- Checking that any information that they provide to the College in connection with their course is accurate and up to date;
- Informing the College of any changes to information, which they have provided e.g. changes of address, contact numbers, names etc.;
- Informing the College of any errors or changes. However, the College cannot be held responsible for any errors unless the employee has informed the College of them.

6. Responsibilities: Visitors

6.1 Visitors are guests who attend the College premises for a temporary period of time, and who are not employed by or enrolled at the College, are required to check that any information provided to the College in respect of their visit is accurate and up to date.

7. Notification of data held and processed

7.1 All employees, students and other users are entitled to:

- Know what information the College holds and processes about them and why;
- Know how to gain access to it;
- Know how to keep it up to date;
- Know what the College is doing to comply with its obligations under the Data Protection Act.

The College will not automatically provide students with a standard form of notification, which identifies the types of data the College holds on them. It will however, make information known to current students on request.

8. Rights to access information

8.1 Employees, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files.

8.2 In order to gain access, an individual may wish to receive notification of -the information currently being held and this request should be made in writing and pass it to the designated data controller. A standard 'Access to Data' form is attached to this policy (Appendix 2) and pass it to the designated data controller.

8.3 The College will make a charge of £10.00 on each occasion that access is requested, although the College will have discretion to waive this.

8.4 The College aims to comply with all requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 days unless there is good reason for delay. In such cases, the reason(s) for delay will be explained in writing to the data subject making the request.

9. Publication of College information

9.1 Information that is already in the public domain is exempt from the Data Protection Act. It is College policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- Names and contact details of College governors;
- List of employees (names only);
- Photographs of key employees, where possible.

9.2 The College internal phone directory will not be a public document.

9.3 Any individual who has good reason for wishing details or images in these lists or categories to remain confidential should contact the designated data controller.

9.4 The College is also required by various Acts of Parliament and other legislation to disclose personal information to third parties, particularly government departments. For example it has a duty under the Further and Higher Education Act 1992 to give information to the Department for Business Innovation and Skills and it has duties under health and safety legislation to report serious accidents.

9.5 The College also fulfils its vision of 'creating a safe and secure environment for students, employees and visitors' through a policy of co-operation with

reasonable requests from the local police when investigating suspected crimes.

9.6 The College discloses these recipients in its Data Protection Register and will ensure that the use of this information is made known to subjects when collected. The College will also ensure that these requests are legal and reasonable by:

- Asking the organisation requesting the information to ask for it in writing;
- Asking for a reason why the information is necessary;
- Seeking the approval from the designated data controllers for releasing the information, where possible.

10. Subject consent

10.1 In many cases, the College can only process personal data with the consent of the individual. However, the College also has important safeguarding responsibilities to both employees and students and must therefore ensure that all employees and those who use the College's facilities do not pose a threat or danger to other users. Therefore, if the data is sensitive, express consent must be obtained.

10.2 Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student on to any course, and a condition of employment for employees. This includes information about previous criminal convictions through the Disclosure and Barring Service.

10.3 Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 14-18. The College follows safer recruitment principles to ensure that all employees are suitable to work with children, young people and adults at risk.

10.4 The College also asks new employees for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma and diabetes. The College 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.

11. Processing sensitive information

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

11.2 As this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, employees and students will be asked to give consent for the College to do this.

11.3 Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the designated data controller.

12. The data controller and the designated data controller(s)

12.1 Lewisham Southwark as a corporate body is the data controller under the Data Protection Act, and the Governing Body is therefore ultimately responsible for the implementation of the Act. However, designated data controllers will deal with the day to day matters.

12.2 The College has two designated data controllers. They are:

- **Sue Glover, Clerk to the Corporation: 020 3757 4496 (All matters excluding employee related issues)**

- **Jean Inker, Interim Director of HR: 020 3757 3670 (Employee related issues)**

12.3 Compliance with the Data Protection Act is the responsibility of all employees and students of the College. Any deliberate breach of the Data Protection policy may lead to disciplinary action being taken, access to College facilities being withdrawn, or even to a criminal prosecution.

12.4 Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated data controller.

13. Qualifications

13.1 Students will be entitled to information about their marks both for coursework and examinations. However, this may take longer than other information to provide in some circumstances.

13.2 The College may withhold certificates, accreditation or references in the event that the full-time course fees have not been paid, or all books and equipment have not been returned to the College.

13.3 This measure will only be used where it is reasonable and where the student has been given every chance to pay the outstanding fee or return the books or equipment.

14. Retention of data

14.1 The College will keep some forms of information for longer than others. The College will aim to keep a simple record for all students, identifying their basic enrolment details (name, address and course) and whether they have completed or passed their qualification. The College will aim to keep this information indefinitely, but does not have a complete set of data on past students.

14.2 The College will aim to keep other relevant information (for example on attendance and references) for a period of ten years so that it can answer queries on former students progressing to jobs which require a 10 year career history. All other information, including any information about health, race or disciplinary matters will be destroyed within five years of the course ending and the student leaving the College.

14.3 The College may need to keep information about employees for longer periods of time. In general information that is of genuine relevance or importance will be kept for 10 years after an employee leaves the College. Some information however is kept for much longer. This will include information in respect of pensions, taxation, potential or current disputes or litigation regarding the employment and job references.

14.4 The College will aim not to retain data that are held for a particular purpose once that purpose no longer exists.

14.5 A full list of information with retention times is available from the data controller.

15. Reporting of achievement of/compliance with the policy

15.1 This policy will be reviewed and amended in line with changes to legislation and/or College procedures. Where relevant, compliance will be monitored by the HR Department. Comments or suggestions about this policy should be referred to the HR Department in the first instance.

16. Linked policies and procedures

16.1 This policy is linked to the following policies:

- Disciplinary policy and procedure;
- Recruitment and Selection policy and procedure.

17. Impact assessment

17.1 This policy was impact assessed on: date to be confirmed

Approved by:	Board of Governors	March 2016
Publication date:	April 2016	
Review date:	October 2018	

Appendix 1

Employee Guidelines for Data Protection

1. All employees will process data about students on a regular basis, when marking registers, or College work, writing reports or references, or as part of a pastoral or academic supervisory role. The College 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 (updates in 2003).

2. The information that employees 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/or discipline.

3. 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 student's consent.

   Examples: 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 personal duties.

4. All employees have a duty to make sure that they comply with the data protection principles, which are set out in the College Data Protection policy. In particular, employees must ensure that records are:

   - Accurate;
   - Up-to-date;
   - Fair;
   - Kept and disposed of safely and in accordance with the College policy.

5. The College will designate members of employees as 'authorised employees'. These are the only employees authorised to hold or process data that are:

   - Not standard data (as defined in 1 above), or
   - Sensitive data (as defined in 2 above).

6. The only exception to this will be if a non-authorised employee is satisfied that the processing of the data is necessary, in the best interests of the student or employee, or a third person, or the College and s/he has either

informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances. This should only happen in very limited circumstances.

Example: A student is injured and unconscious, but in need of medical attention, and an employee tells the hospital that the student is pregnant or a Jehovah's Witness.

7. Authorised employee will be responsible for ensuring that all data are kept securely.

8. Employees must not disclose personal data to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with the College policy.

9. Employees must not disclose personal data to any other employees except with the authorisation or agreement of the designated data controller, or in line with College policy.

10. Before processing any personal data, all employees should consider the checklist below.

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 data subject been told that this type of information will be processed?
- Are you authorised to collect/store/process the data?
  If yes, have you checked with the data subject that the data are accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied?
- Is it in the best interests of the data subject to collect and retain the data?
- Have you discussed any concerns you may have with the Data controller?

Appendix 2

Standard request form for access to data

To the Data Controller:

I, (insert your name) …..... wish to have access to either (delete as appropriate):

1. All the data that the College currently holds on me, either as part of an IT system or part of a relevant filing system; **or**

2. Data that the College has about me in the following categories:

    - Academic marks or course work details
    - Academic or employment references
    - Disciplinary records
    - Health and medical matters
    - Political, religious or trade union information
    - Any statements of opinion about my abilities or performance
    - Personal details including name and address, date of birth etc.
    - Other information

    (Please tick as appropriate)

I understand that I will have to pay a fee of £10.00 and provide that sum by cheque in order that the access request can be commenced.

Signed .....

Dated .....