SOUTH LONDON ACADEMY

Data Protection Policy

Document Control Summary

Document number: SLA23 v1.0

Date created / revised: August 2016

Date of approval: Sept 2016

Approved by: Senior Management Team

Date of Next review: Dec 2018

Next review date: Dec 2018

Data Protection Policy

Data Protection

1: Scope / Requirements The Academy needs to keep certain information about employees, students and other individuals in order to perform its business duties. The Academy also needs to process information so that employees can be recruited and paid, and legal obligations are complied with.

To comply with the law, all information must be used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Academy must comply with the Data Protection Act 1998 and work with our partner awarding bodies such as the ATHE, City & Guilds and other regulatory authorities in its implementation. The Act is governed by four codes covering recruitment & selection, manual or computer records, monitoring at work and medical information. Anyone processing personal data must comply with eight enforceable principles of good practice.

2: Principles of Data Protection

The principles state that data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Kept no longer than is necessary;
- Processed in accordance with the data subject's rights;
- Secure.

Data must not:

- Be transferred to countries without acceptable data protection laws unless explicit prior consent has been obtained.

Personal data covers both facts and opinions about you as an employee. It also includes information regarding the intentions of the data controller towards employees although in some limited circumstances, exemptions will apply. Processing data incorporates the concepts of obtaining, holding and disclosing personal information.

The Academy will hold and otherwise process data for the following principal purposes:

- Recruitment, promotion, training, redeployment and/or career development;
- Payroll data, including details of bank and building society accounts and wage transfers;
- Contacting next of kin and arranging medical attention in connection with death, illness

and injury whilst at work;

- Compliance with statutory and other requests from relevant public authorities such as Inland Revenue or the Benefits Agency;
- Disciplinary purposes arising from an employee's conduct or ability to perform job requirements;
- Undertaking reasonable monitoring of employees;
- The provision of references following a request from you or a potential employer, subject to your consent.

3: External data processing

Data may be made available to the Academy's suppliers in connection with any legitimate data processing purposes. An example would be third parties administering schemes such as a pension scheme.

4: Your responsibilities

You are responsible for:

- Checking that any information provided to the Academy is accurate and up to date;
- Informing the HR Manager of any changes to your personal information e.g. change of address or next of kin;
- Informing the HR Manager of any errors or changes in information.

The Academy cannot be held responsible for any such errors unless you have informed HR accordingly. If and when, as part of your duties, you collect information about other people, you must comply with the Data Collection Guidelines outlined in this section.

5: Data security

You are responsible for ensuring that:

- Any data which you hold is kept securely (eg. using a locked filing cabinet or drawer, or using passwords to protect computer documents, or kept only on disk which itself is kept securely)
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised party.

6: Access to information

You have a right to be informed where personal data is being processed, where the data is being held, the purpose of the processing and the persons to whom the data may be disclosed. You should make such requests in writing to the HR Manager. The information will then be supplied to you within 40 days of the Academy receiving your request.

7: Your consent

In many cases, we can only process personal data with your prior consent. In some cases, if the data is sensitive, express consent must be obtained. Therefore, all prospective employees will be asked to consent to their data being processed on application for employment.

8: Data Controller

The Academy is the data controller under the Act, and is ultimately responsible for implementation. However, designated data controllers will deal with day to day matters. The designated data controller in the Academy is the Registrar.

9: Retention of data

Employee data which is no longer accurate, relevant or up to date will be destroyed. However, some HR information may be retained indefinitely. This will include information in respect of, for example, taxation, potential or current disputes regarding employment, and information required for job references. Compliance with the Data Protection Act 1998 is the responsibility of all employees. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or even a criminal prosecution. Any questions or concerns regarding this policy should be referred to the Registrar.

10: Data collection guidelines

Personal Data will be processed on a regular basis. You should ensure that data subjects give their consent to processing and are notified of the categories of processing, as required by the Act. Information about an individual's physical or mental health, sexual life, political or religious views, trade union membership, ethnicity or race is sensitive and can only be collected or processed with the individual's express consent.

You are responsible for ensuring that all data you are holding (either manually or on computer) is kept securely. You should not disclose personal data, unless for administrative purposes, without authorisation or agreement from the HR Manager. Before processing data, you should consider the following checklist:

- Do you really need to record the information?
- Is the information standard or sensitive?
- If it is sensitive, do you have the data subject's express consent?
- Has the individual or data subject been told how their data will be processed?
- Are you authorised to collect, store or 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 their best interests to collect and retain the data?
- How long do you need to keep the data for, and what is the mechanism for review or destruction?