LOOE COMMUNITY ACADEMY TRUST

DATA PROTECTION POLICY

Introduction

1. Looe Community Academy Trust (the Academy) is required to maintain certain personal data about living individuals for the purposes of satisfying operational and legal obligations. The Academy recognises the importance of the correct and lawful treatment of personal data as it maintains confidence in the organisation and provides for successful business operations.

2. The types of personal data that the Academy may require include information about current, past and prospective employees (including volunteers and governors), students, suppliers and others with whom it communicates. This personal data, whether it is held on paper, on computer or on other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Act 1998.

3. The Academy fully endorses and adheres to the eight principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transporting and storing of personal data. Employees and any others who obtain, handle, process, transport and store personal data for the Academy must adhere to these principles.

Principles

4. The principles require that personal data shall:

- Be processed fairly and lawfully and shall not be processed unless certain conditions are met;
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
- Be adequate, relevant and not excessive for those purposes;
- Be accurate and, where necessary, 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 secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures;
- Not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Satisfaction of principles

5. In order to meet the requirements of the principles, the Academy will:

- Observe fully the conditions regarding the fair collection and use of personal data;
- Meet its obligations to specify the purposes for which personal data is used;
- Collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
- Ensure the quality of personal data used;
- Apply strict checks to determine the length of time personal data is held;
- Ensure that the rights of individuals about whom the personal data is held can be fully exercised under the Act;
- Take the appropriate technical and organisational security measures to safeguard personal data;

Policy approved by the Board June 2013. Next review due Summer term 2015.

The Academy's Data Controller

6. The Academy's Governing Body is the registered Data Controller.

Roles and responsibilities

7. The Academy's Governing Body is corporately responsible for ensuring compliance with the Data Protection Act and for reviewing the effectiveness of this policy and the supporting procedures, amending as necessary to incorporate good practice.

8. The Business Manager is responsible for championing data protection across the Academy and for ensuring the implementation of and compliance with this policy.

9. Leaders and line managers at all levels are responsible for ensuring that their staff are suitably conversant with the data protection requirements for their job role and for arranging training as necessary.

Status of the policy

10. This policy has been approved by the Governing Body and any breach will be taken seriously and may result in disciplinary action.

11. Any employee who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Business Manager or the Headteacher.

Definitions

12. For the purposes of this policy, the following definitions apply:

- "Personal data" means data that relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so too can names and photographs, if published in the press, internet or by the media;
- "Processing" means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data;
- "Data subject" means an individual who is the subject of personal data or the person to whom the information relates;
- "Parent" has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

Subject access

13. All individuals who are the subject of personal data held by the Academy are entitled to:

- Ask what information the Academy holds about them and why;
- Ask how to gain access to it;
- Be informed how to keep it up to date;
- Be informed what the Academy is doing to comply with its obligations under the Data Protection Act 1998.

Employee responsibilities

14. All employees are responsible for:

- Checking that any personal data that they provide to the Academy is accurate and up to date;

- Informing the Academy of any changes to information that they have provided, e.g. changes of address;
- Checking any information that the Academy may send out from time to time giving details of information that is being kept and processed.

15. If, as part of their responsibilities, employees collect information about other people (e.g. personal circumstances, or about employees), they must comply with this Policy and with the Academy's Data Protection practices.

Data security

16. The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely;
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Rights to access information

17. Employees, students and other subjects of personal data held by the Academy have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in certain manual filing systems. This right is subject to certain exemptions which are set out in the Data Protection Act. Any person who wishes to exercise this right should make the request in writing to the Headteacher.

18. The Academy reserves the right to charge the maximum fee payable for each subject access request. If personal details are inaccurate, they can be amended upon request.

19. The Academy aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a written request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

Publication of Academy information

20. Information that is already in the public domain is exempt from the 1998 Act. This would include, for example, information on staff contained within externally circulated publications such as the Academy Prospectus. Any individual who has good reason for wishing details in such publications to remain confidential should contact the Headteacher.

Subject consent

21. The need to process data for normal purposes has been communicated to all data subjects. In some cases, if the data is sensitive, for example information about health, race or gender, express consent to process the data must be obtained. Processing may be necessary to operate Academy policies, such as health and safety and equal opportunities.

Retention of personal data

22. The Academy will keep some forms of information for longer than others. All staff that process data are responsible for ensuring that information is not kept for longer than necessary.

23. The Academy has a duty to retain some staff and student personal data for a period of time following their departure from the Academy, mainly for legal reasons, but also for other purposes such as being able to provide references and academic transcripts, or for financial reasons, for example relating to audit, pensions and taxation. Different categories of data will be retained for different periods of time.

Disposal of personal data

24. When a record containing personal data is to be disposed of, the following procedures will be followed:

- All paper or physical documentation containing personal data will be permanently destroyed by shredding;
- All computer equipment or media that are to be reallocated internally, sold or scrapped will have had all personal data completely destroyed, by reformatting, over-writing or degaussing.

25. Employees and, where appropriate, students, will be provided with guidance as to the correct mechanisms for disposal of different types of personal data and audits will be carried out to ensure that this guidance is adhered to. In particular, employees will be made aware that erasing or deleting electronic files does not equate to destroying them. Guidance can be obtained from support@looe.cornwall.sch.uk.

Annexes:

A. Looe Community Academy Trust - Data Protection Code of Practice.
B. Looe Community Academy Trust - Disclosure and Transfer of Personal Data.
C. Looe Community Academy Trust - Access to Personal Data Request Form.

Annex A

LOOE COMMUNITY ACADEMY TRUST

DATA PROTECTION CODE OF PRACTICE

Introduction

1. This Code of Practice must be read in conjunction with the Academy's Data Protection Policy document to give the fullest picture of the Academy's data protection regime. This Annex gives an introduction to some basic points of practice relating to the handling and processing of personal data.

Key concepts

2. The Data Protection Act 1998 places an obligation upon the Academy, as a data controller, to collect and use personal data in a responsible and accountable fashion. The Academy is committed to ensuring that every current employee and registered student complies with this Act to ensure the confidentiality of any personal data held by the Academy in whatever form. Three key concepts to be considered are those of purpose, fairness and transparency.

Purpose

3. Data controllers can only process personal data where they have a clear purpose for doing so and then only as necessitated by that purpose. The Academy publishes the purposes for which the Academy processes personal data. Personal data cannot be processed for purposes that have not been defined and declared by the Academy. The Academy Trust, as Data Controller, has registered its purposes with the Information Commissioner and details can be found at www.ico.org.uk/esdwebpages/search using registration number Z3034634.

Fairness

4. In defining the purposes for which the Academy processes personal data, the fairness of that processing must be considered. For some types of processing the required elements of fairness and legality are clearly outlined in the legislation.

Transparency

5. Members of staff, students and others must be able to feel that there is no intention to hide from them details of how their personal data are collected, used and distributed by the Academy. One of the functions of this Code of Practice is to provide that assurance.

Collection and amendment of personal data

6. In most cases, the personal data held by the Academy will be obtained directly from the data subjects themselves. The law stipulates that a data protection notice must accompany any request for personal data. Any members of staff responsible for managing the collection of personal data for the legitimate activities of the Academy must ensure that a notice containing the following information is included in the request for that data:

- A statement that the Academy is the data controller;
- The name and or job title of the specific member of staff responsible for the administration of the personal data being collected, to enable, for example, subsequent amendments to be submitted by the data subject;

- A clear explanation of the types of data being collected and the purposes for which that data will be processed;
- Any further information that is considered necessary to ensure that the data processing can be described as being fair, for example details of any third parties to whom the data might be disclosed;
- A statement making it clear that by submitting the personal data, the data subjects are giving their consent for the processing of the data for the stated purposes to take place.

7. From time to time data subjects will wish to update some of their personal data held by the Academy, for example their home addresses or other contact details previously submitted. To do this, the data subjects must either contact the specific member of staff designated in the data protection notice at the time the data was submitted.

Security of personal data

8. Of fundamental importance within any data protection regime is the security of the personal data that is being processed. Data subjects have the right to expect that their personal data will be kept and processed securely and that no unauthorised disclosures or transfers will take place to anyone either within or outside the Academy. Authorised disclosures or transfers are those that are defined within the appropriate notifications and declared to the data subject either at the point of data collection or subsequently, the necessary consent for disclosure or transfer having been obtained if required. To help ensure the security of personal data within the Academy, all those who process such data in the course of performing their duties are required to follow the general guidelines set out below.

Secure storage of personal data

9. Each member of staff whose work involves storing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage, in line with the Data Protection Policy, which states that personal data should:

- Be kept in a locked filing cabinet, drawer, or safe;
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up;
- If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

10. Ordinarily, personal data should never be stored at a staff member's home, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites.

11. Staff should be aware that log files record details of all users who access, alter or delete or attempt to access, alter or delete centrally held computerised databases and files containing personal data.

Secure processing of personal data

12. While staff members in the course of performing their legitimate duties are using personal data, reasonable precautions must be taken to ensure the safety and privacy of that data. For example:

- In open-plan offices or offices with windows, computer screens that could potentially be displaying personal data should not be positioned such that unauthorised staff or visitors may readily see that data;
- Password-protected screensavers should be activated when computers are not being used;

- Personal data in manual form, such as in paper files, correspondence or database printouts, should not be left in view in open-plan offices or offices with windows while the relevant staff members are away from their desks. They should instead be locked away or at least covered;
- Where manual records containing personal data are accessible to a number of staff in the course of their legitimate activities, access logs should be used where practicable to help monitor the whereabouts and use of such records.

13. Ordinarily, personal data should not be processed at a staff member's home, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the relevant Senior Leader must be obtained, and all the security guidelines given in this document must still be followed.

Annex B

LOOE COMMUNITY ACADEMY TRUST

DISCLOSURE AND TRANSFER OF PERSONAL DATA

Authorised and unauthorised disclosures

1. If they are unclear, staff members working with personal data will seek advice from their line manager or other appropriate staff as to the purposes for which the data is processed and the legitimate parties either within or outside the Academy to whom that data, either in whole or in part, may be disclosed or transferred.

2. Personal information must not be disclosed either orally or in writing or via web pages or by any other means, manual or electronic, accidentally or otherwise, to any unauthorised third party.

3. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

4. Any unauthorised disclosure must be reported to the Business Manager as soon as it is identified.

Security of data during transfer

5. Where personal data is transferred between staff members within the Academy in the course of their legitimate activities, the level of security appropriate to the type of data and anticipated risks should be applied. For example, sensitive personal data should either be transferred by internal mail in sealed envelopes or by hand. If transferred by e-mail, such data should normally either be encrypted or sent in a password-protected attachment (for example using Microsoft Word's "require password to open" feature), with the password being supplied separately.

Disclosures outside the Academy

6. When a request to disclose or amend personal data relating to a member of the Academy (students or staff) is received from an individual or organisation outside the Academy, in general no data should be disclosed or amended unless the authority and authenticity of the request can be established. Disclosures requested by those claiming to be relatives or friends should be refused unless the consent of the data subject is obtained for such disclosures or in one of the few situations where disclosure without consent is permitted by the law.

7. Requests for the disclosure of personal data from the Police, Government bodies or other official agencies should be investigated sufficiently to verify the authenticity of the request and may then be acted upon if there is a legal requirement for such disclosure or the consent of the data subject has been given for the disclosure.

Publication of Academy Information

8. While the majority of personal data held by the Academy is processed for internal administrative purposes and is never disclosed outside the institution, some categories of data are routinely or from time to time released through one or more forms of publication.

Legal obligations

9. When required by law or statute, the names of staff and Governors of the Academy and certain other personal data relating to employees and Governors are published in documents and on the website,

for example, the Academy's annual audit report. The Academy also fulfils all obligations placed upon it by its relationship with various funding bodies, Government agencies and the like with regard to the release of personal data and statistical information concerning students and staff. Data subjects will be informed of the Academy's obligations in this respect.

Staff directory

10. In order to meet the legitimate needs of parents, visitors and enquirers to be able to make contact with appropriate staff, the Academy intends to make available on its public website a directory containing the job title, organisational unit, title, forename, surname, office telephone number, office room number and office e-mail address of each staff member.

Student personal data

11. Apart from the obligations mentioned above, the Academy will not ordinarily reveal any personal details of students enrolled at the Academy to any individual or body outside the Academy.

Annex C

LOOE COMMUNITY ACADEMY TRUST

ACCESS TO PERSONAL DATA REQUEST FORM

Data Protection Act 1998 - Section 7

1. Enquirer's Details:

Surname		Salutation	
Forenames			
Address			
Postcode		Telephone	

2. Are you the person who is the subject of the records you are enquiring about (i.e. the "data subject")? YES / NO (if YES then go to 5)

3. If NO to 2, do you have parental responsibility for a child who is the "data subject" of the records you are enquiring about? YES / NO

4. If YES to 3, please provide the name and date of birth of child or children about whose personal data records you are enquiring:

	Name (include all names used by the student while at the Academy)	Date of Birth
a.		
b.		
c.		
d.		

5. Description of enquiry:

6. Description of any specific information or topic requested:

7. Please provide any additional Information to support your request:

8. Data Subject Declaration:

I request that the Academy searches its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provides a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the Academy.

I agree that the reply period will commence when I have supplied sufficient information to enable the Academy to perform the search and, where appropriate, when payment has cleared.

I consent to the reply being disclosed and sent to me at the address stated above.

Signature of "data subject" (or subject's parent or person with parental responsibility)	
Name of "data subject" (or subject's parent or person with parental responsibility) (please print)	
Date submitted	

For office use only:

Date received	
Details of any further information/clarification sought	
Validity of request authorised by	
Payment required?	
Payment of £____ requested on	
Payment received on	
Request to be actioned by	
Target date for response	
Date of response	