Connect Academy Trust

Data Protection Policy

For Review and Approval by the Directors of Connect Academy Trust

Version 2 – 19/4/17

Amendments

Version	Date	Detail
1	16/3/17	Newly created policy
2	19/4/17	Renamed Data Protection from Personal Data Protection. Appendices attached

Contents

Data Protection Policy

This document is a statement of the aims and principles of the Connect Academy Trust (the Trust), for ensuring the confidentiality of personal data and sensitive personal data relating to staff, pupils, parents/carers and governors.

1. Introduction

1.1 The Trust and its schools need to keep personal data about its employees, students and other users to allow it to monitor performance, achievements, health and safety, to process data so that staff can be safely recruited and paid, to manage the professional development of staff and to discharge other functions associated with the provision of education. In addition there may be legal requirement to collect and process personal data to ensure that the Trust and its schools comply with statutory obligations.

1.2 To do this, the Trust must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (DPA). In summary these 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 shall not be processed in any manner incompatible with that purpose;
- be adequate, relevant and not excessive for that purpose;
- 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.

1.3 The Trust and all staff or others who process or use personal data must ensure that they follow these principles at all times. In order to ensure that this happens, Connect Academy Trust has developed this Data Protection Policy.

2 Status of this Policy

2.1 This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the Trust from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

3. The Data Controller and the Designated Data Controllers

3.1 The Trust as a body corporate is registered as a Data Controller with the Information Commissioners Office (ICO). Schools that are members of the Trust are also named in the registration as Data Controllers. As such, the Governors of each school are responsible for ensuring the requirements of the DPA are implemented at establishment level. However, the Designated Data Controllers at each school will deal with day to day matters.

3.2 The Trust has a Designated Data Controller (the CEO), and this is the named person in the notification to the Data Protection Commissioner.

4. General Statement

4.1 The Trust is committed to maintaining the above principles at all times. Therefore the Trust and its schools will:

- inform individuals why the information is being collected when it is collected;
- inform individuals when their information is shared, and why and with whom it was shared;
- check the quality and the accuracy of the information it holds;
- ensure that information is not retained for longer than is necessary;
- ensure that when obsolete information is destroyed that it is done so appropriately and securely;
- ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- share information with others only when it is legally appropriate to do so;
- set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests;
- ensure our staff are aware of and understand our policies and procedures

5. Fair and Lawful Processing

5.1 The Trust and its schools will usually only process your personal data where you have given your consent or where the processing is necessary to comply with our legal obligations. In other cases, processing may be necessary for the protection of your vital interests, for our legitimate interests or the legitimate interests of others. The full list of conditions is set out in the DPA.

5.2 "Personal data" means recorded information we hold about living individuals from which they can be identified. It may include contact details, other personal information, photographs and expressions of opinion or indications as to our intentions about individuals.

5.3 "Processing" means doing anything with the data, such as accessing, disclosing, destroying or using the data in any way.

5.4 The Trust and its schools will only process "sensitive personal data" about ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, sex life, criminal proceedings or convictions, where a further condition is also met. Usually this will mean that you have given your explicit consent, or that the processing is legally required for employment purposes. The full list of conditions is set out in the DPA.

6. How We Use Personal Data

6.1 The Trust and its schools will process data about staff for legal, personnel, administrative and management purposes in order to enable us to meet our legal obligations as an employer, for example to compensate you, monitor your performance and to confer benefits in connection with your employment.

6.2 The Trust and its schools may process sensitive personal data relating to staff including, as appropriate:

- information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions related to the employee's fitness for work;
- the employee's racial or ethnic origin or religion or similar information in order to monitor compliance with equal opportunities legislation;
- in order to comply with legal requirements and obligations to third parties;
- in order to discharge its duty of care to all staff and students and to make sure that employees and those who use school facilities do not pose a threat or danger to other users;
- information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The school will only use this information in the protection of the health and safety of the individual (consent will be required to process this data) to allow the disclosure of information to health professionals in the event of a medical emergency, for example.

7. Processing Sensitive Information

7.1 Sometimes it is necessary to process information about a person's health, criminal convictions and race. This may be to ensure that the Trust is a safe place for everyone, or to operate other Trust policies, such as the Sick Pay Policy or the Equal Opportunities Policy. Because this information is considered sensitive under the 1998 Act, staff (and students where appropriate) will be asked to give their express consent for the Trust to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

8. Processing for Limited Purposes

8.1 The Trust and its schools will only process your personal data for the specific purposes notified to you via our Privacy Notice, or in circumstances where specifically permitted by the DPA. We will notify you of the purposes that personal data will be processed for via a Privacy Notice that will be published on the websites of the Trust and its schools.

9. Adequate, Relevant and Non-Excessive Processing

9.1 Your personal data will only be processed to the extent that it is necessary for the specific purposes notified to you.

10. Accurate Data

10.1 The Trust and its schools will keep the personal data we store about you accurate and up-to-date. Data that is inaccurate or out-of-date will be destroyed. Please notify us if your personal details change or if you become aware of any inaccuracies in the personal data we hold about you.

11. Data Retention

11.1 The Trust and its schools has a duty to retain some staff and student personal data for a period of time following their departure from the Trust, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

11.2 The Trust and its schools will not keep your personal data for longer than is necessary for the purpose it was originally collected for. This means that data will be destroyed or erased from our systems when it is no longer required.

12. Processing in Line With Your Rights

12.1 You have the right to:

- request access to any personal data we hold about you;
- prevent the processing of your data for direct-marketing purposes;
- ask to have inaccurate data held about you amended;
- prevent processing that is likely to cause unwarranted substantial damage or distress to you or anyone else;
- object to any decision that significantly affects you, being taken solely by a computer or other automated process.

13. Data Security

13.1 The Trust and its schools will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

13.2 The Trust and its schools have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. We will only transfer personal data to a third party if the third party agrees to comply with those procedures and policies, or if they put in place adequate measures themselves.

13.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

14. Providing Information to Third Parties

14.1 The Trust and its schools will not disclose your personal data to a third party without your consent, unless we are satisfied that they are legally entitled to the data. Where we do disclose your personal data to a third party, we will have regard to the eight data protection principles.

15. Subject Access Requests

15.1 All staff, parents and other users have a right under the DPA to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should complete the Subject Access Request Form (Appendix 1) and submit it to the Designated Data Controller.

15.2 The Trust/school will, upon receipt of a written request, acknowledge receipt and confirm any additional information or payment that may be required in order to process the request. Trust/school to complete Subject Access Request Checklist (Appendix 2)

15.3 The school will normally make a charge of £10 on each occasion that access to personal data is requested, although the school has discretion to waive this.

15.4 The Trust/school aims to comply with requests for access to personal data as quickly as possible, but will ensure that it is provided within statutory 40 day timescale.

16. Responsibilities of Staff

16.1 All staff are responsible for:

- checking that any information that they provide to the school in connection with their employment is accurate and up to date;
- informing the school of any changes to information that they have provided, eg. change of address, either at the time of appointment or subsequently. The school cannot be held responsible for any errors unless the staff member has informed the school of such changes.

16.2 If and when, as part of their responsibilities, staff collect information about other people eg. about a student's homework, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in the school's Code of Conduct and/or ICT Acceptable Use Policy.

16.3 All staff are responsible for ensuring that data security is maintained in line with the Trust policies. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

16.4 Staff must ensure that where possible personal data is:

- not transferred outside of the Trust/school networks through non-secure/encrypted email addresses;
- kept in a locked filing cabinet, drawer, or safe; and only made available where there is relevant/appropriate purpose to do so, or;
- if it is computerised, be stored on an appropriate location on the Trust/school local network drive that is regularly backed up; or; in an approved cloud storage system with security authentication, or;
- if personal data is held on a laptop, mobile device or other removable storage media, that media must itself be encrypted to required data security standards and kept in a locked filing cabinet, drawer, or safe when not in use.

17. Publication of Connect Academy Trust Information

17.1 Certain items of information relating to Trust staff will be made available via searchable directories on the public website, in order to meet the legitimate needs of researchers or visitors.

18. Complaints/Breaches of this Policy

18.1 If you consider that this policy has not been followed in respect of personal data about others, you should raise the matter with the school office. Any breach of this policy will be taken seriously and may result in disciplinary action.

18.2 Any member of staff, parent/carer or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the

matter with the appropriate Designated Data Controller, or the Headteacher. Any breach of this policy will be taken seriously and may result in disciplinary action.

Appendix 1

Subject Access Request Form

Data Protection Act 1998

The following information is needed to help provide a quick and accurate response to your enquiry. Please complete the information below and return the form by post or email to Mrs J Bellamy, Data Protection Officer and CEO of Connect Academy Trust.

Leigham Primary School, Cockington Close, Leigham, Plymouth, PL6 8RF

admin@leigham-primary.plymouth.sch.uk

Telephone - 01752 790990

1. **Your Request**

Title	
Surname	
Forename(s)	
Address	
Telephone number	
E-mail address	
Other name by which you have been known, if applicable	
Relationship to the Academy	

Please provide a description of your request and any further information which will enable us to locate your personal data (continue overleaf if necessary).

2. **Proof of Identity**

The Data Protection Act requires the academy to satisfy itself as to the identity of the person making the request. Please send a photocopy of one form of identification containing a photograph (eg. Passport, Photocard Driving Licence) to the Data Protection Officer. If the supply of this documentation is problematic please contact us to discuss alternative proof of identity arrangements. If the Academy is unable to satisfy itself as to your identity from the documentation you send us, we will contact you as soon as possible.

3. **Fee**

The Academy charges a statutory fee of £10 to process subject access requests. Payment may be made by one of the following methods:

Cash – but only if you are submitting your request in person to the Academy's Reception during office hours at the address given on the first page of this form (please note that you will not be able to discuss the content of your request in person and furthermore the Data Protection Officer may not be available to receive your request themselves).

BACS payment – bank details can be provided on request.

4. **Declaration**

I am the Data Subject named in Part 1 of this document, and hereby request, under the provisions of Section 7(1) of the Data Protection Act 1998, that the Academy provides me with copies of my personal data as described in Part 1.

I have provided my proof of identity and have paid/enclose the £10 fee.

Signature: ……

Date: …….....

Appendix 2

Subject Access Request Checklist

Step 1 – Validate the Request	

1.	**Check Identity**
Q	Are you satisfied that the person is who they say they are?
You can ask for sufficient information from the requester to enable you to confirm their identity. This is because you must only disclose personal information to the individual (or their representative – see 2. below)	
Note	Do not discuss a request, or whether you do or do not hold personal information, until you are satisfied of the requester's identity. This is because even confirming that personal information is held could divulge information about someone.

2.	**Check Authority**
Q	Are you satisfied that the person has the authority to make a request on behalf of someone else?
This will be relevant when someone is (a) asking to see someone else's personal information, or (b) is explicitly claiming to make a request on behalf of someone else.	
No individual has an automatic right under the Data Protection Act to request access to someone else's personal information. However, someone can agreed to a representative making a request for them (eg. a parent for a child; a solicitor for their client; where there is power of attorney). You therefore need to check this agreement.	

3.	**Check Request**
Q	Do you have enough information to locate what is being requested?
You can ask for sufficient detail from the requester to enable you to locate the personal information they are seeking. This is because people only have a right of access to their own personal information.	
eg.	If you have personal information for a number of people with the same name, you could ask for further details from the requester (eg. date of birth) to distinguish them from the other people.
eg.	If the request is for 'all personal information' you could ask whether any specific information might satisfy the request, or that could be processed first.

4.	**Check Payment**
Q	Are you going to ask for £10 to process the request?
You are entitled to charge £10 for processing a Subject Access Request.	
Q	If so, have you received payment?
You do not *have* to start processing the request until you have received payment.	

Step 2 – Locate the Personal Information

Electronic system name	Search undertaken		Result	If no personal information has been located – document any possible rationale
	Names	Dates / range of dates		

Employee consulted	Search undertaken	Result	If no personal information has been located – document any possible rationale

Hardcopy (paper) filing system name	Search undertaken	Result	If no personal information has been located – document any possible rationale

Step 3 – Review the Personal Information

Once the personal information subject to the request has been located, it must be reviewed.

Review of Third Party Personal Information		
The following should be considered for <u>each piece</u> of third party personal information:		
1. Can you disclose the personal information without disclosing information relating to, or identifying, anyone else? Note. You should consider not only the information you are about disclose, but also whether the information could be used with any other information you think the requester might have (or be able to get).	**Yes**	**No / unsure**
	Include the third party personal information in the response. *Continue to 6*	*Continue to Q2 below*
2. Are the third party's details simply not part of the request? ie. the third party's name and information are unrelated to the requester. For example, on a list of attendees or list of names and addresses.	**Not part of the request**	**Are part of the request (or think they are)**
	Blank out / delete them from the response. *Continue to 6*	*Continue to Q3 below*
If it is not possible to separate the third party information from the personal information of the requester. Consider the questions below:		
3. Can you consult the third party and ask for their consent? Note: You must be sure that the requester is happy for you to approach the third party – ie. because in doing so, you will be informing the third party that the requester has made a request (which in itself could be something the requester wants to keep private).	**No**	**Yes**
	The requester did not want us to, or it is not possible (we do not know where they are) *Continue to Q5*	*Continue to Q4*
4. Has the third party agreed that the personal information which involves them can be disclosed to the requester? Keep a record of the third party's decision – whether there is agreement, or what the rationale is for not providing consent.	**No (or they are incapable of giving consent)**	**Yes**
	Continue to Q5	Include the third party personal information in the response. *Continue to 6*
5. Even without consent, would it be 'reasonable in all the circumstances' to disclose the third party personal information to the requester?		
The following points should be considered:		

(a) Is the third party owed or expecting confidentiality in relation to the personal information in question? ie. because of the nature of the relationship between the third party and the person to whom they disclosed the information.	**No**	**Yes**
	It is likely to be reasonable to include the information in your response.	It is not likely to be reasonable to disclose the information.
(b) Does the requester already know the information in question? ie. because it is common known between the two parties; it is public knowledge it has previously been provided to the requester.	**Yes**	**No**
	It is likely to be reasonable to include the information in your response.	It is not likely to be reasonable to disclose the information.
(c) How significant is the personal information? eg. is it current or historic; very sensitive or minor.	You need to weigh the possible wish to maintain confidentiality against the requester's right to access their personal information.	
(d) What are the circumstances behind both the request and any expected confidentiality?		

6. Summary – Third Party Personal Information

Provide an explanation of the decision you reached. Include references to where the third party personal information was located and the decision reached in each instance.

Document / file name	Location of the third party personal information	Decision	Rationale

Review of possibly exempt personal information

Are there any other reasons for wanting to withhold some or all of the personal information subject to the request?

In general, the threshold for withholding personal information is high – you need a strong reason (or reasons) to justify withholding personal information from someone. For example, if you think that disclosure would be likely to harm a particular function or an individual, the ICO is clear that there should be a "substantial chance (rather than a mere risk) that complying with the [request] would noticeably damage the discharge of the function concerned." Common reasons are outlined below:

a) Crime and taxation	Personal data processed for certain crime and taxation activities; these are: • the prevention or detection of crime; • the capture or prosecution of offenders; and • the assessment or collection of tax or duty.

b) Human Resource issues relating to the requester	ie. confidential references / management information / negotiations
c) Legal advice	ie. information subject to legal professional privilege
d) Social care	ie. where providing access to information about social services, health or education would be likely to cause serious harm to the physical and/or mental health or condition of the requester or any other person.
e) Health records	
f) Education records	

Summary – Exemptions			
Provide an explanation of the decision you reached. Include references to where exemptions were considered and applied, and the rationale in each instance.			
Document / file name	**Location of the third party personal information**	**Decision**	**Rationale**

Step 4 – Respond to the Request

Signed …….
Chief Executive Officer

Date …….

Signed …….
Chair of Operations Committee

Date …….