

Data Protection Policy

September
2016

Date Policy Approved: September 2016

Date Policy to be Reviewed: September 2018

1. Purpose of the Policy

The purpose of the policy is to make staff aware of the data protection act and respect this important legislation in their day to day working. This policy concerns paper records, electronic data on SIMs or IT at whatever location used on behalf of The CLIC Trust.

The obligations outlined in this policy apply to all those who have access to data whether they are governors, employees, employees of associated organisation or temporary staff. It includes those who work from home, who must follow the same procedures as they would in a school environment.

Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or makes an unauthorised disclosure is liable to prosecution. All individuals permitted to access personal data must agree to comply with this policy.

2. Data Protection Act

Schools hold information on pupils and in doing so must follow the requirements of the 1998 Data Protection Act. This means that data held on pupils must only be used for specific purposes that are allowed by the Act. The rules regarding personal data also apply to employees. Schools are 'data controllers' under the Act in that they process 'personal data' in which people can be identified individually.

When data is obtained from data subjects the data controller must ensure, so far as is practicable, that the data subjects have, or are provided with, or have readily available to them, the following information, referred to as the 'fair processing information':

- Details of the data that they hold on them
- The purposes for which they hold the data
- Any third parties to whom the information may be passed.

The DPA updated the rules and regulations on the protection of the individual and extended the principles to apply to all personal data that is processed. The DPA covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data and there are eight principles that must be adhered to as well as a number of conditions that apply. This Act has been

extended to apply to paper files as well as electronic data, so the principles now apply to records and notes that are kept, for example, in teachers' mark books.

The Data Protection Act gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

The second area covered by the Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records. The Data Protection Act doesn't guarantee personal privacy at all costs, but aims to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information.

Each school that processes data must notify the Information Commissioner annually of that fact. If under the previous Act a school's governing body have registered in addition to the headteacher then, under the new Act, there need be only a single registration, and the double entry will need to be corrected.

2.1 Data Gathering

2.1.1 Only relevant personal data may be collected and the person from whom it is collected will be informed why the data is being collected, of the data's intended use and any possible disclosures of the information that may be made.

2.1.2 Privacy notices will be issued to all persons from whom personal data is collected. Two versions will be used – one in respect of students' data collection (Appendix 3) and the other in respect of all other personal data (Appendix 4). These are appended to this policy.

2.3 Processing

2.3.1 All processing of personal data will comply with the Data Protection Principles as defined in the Data Protection Act 1998. In the situation where data is processed by a third party,

the third party will be required to act in a manner that ensures compliance with the Data Protection Act 1998.

- 2.3.2 Data will only be processed for the purpose for which it was collected and will not be used for additional purposes without the consent of the data subject.

2.4 Data Storage

The CLIC Trust will hold the minimum amount of personal data necessary to enable it to perform its functions. The data will be erased once the need to hold it has passed (this will be in line with the regulations around storage and archive of documentation, as per the Records Society)

- 2.4.1 The CLIC Trust will store personal information in a safe and secure manner.
- 2.4.2 Electronic data will be protected by standard passwords and access control systems operated by the CLIC Trust. Any unauthorised access will be monitored and blocked by the firewall and web filtering systems.
- 2.4.3 Computer workstations in administrative areas will be positioned so that they are not visible to casual observers.
- 2.4.4 Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.
- 2.4.5 Particular attention will be paid to the need for security of sensitive personal data.
- 2.4.6 Data protection training and guidance on this policy will form part of the Academy's induction of all new members of staff (and volunteers) where they may have access to any of the personal data it holds

2.5 Data Checking

- 2.5.1 The TMSA will issue annual reminders to staff and parents/carers to ensure that personal data held is up-to-date and accurate.
- 2.5.2 Any errors discovered will be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

2.6 Data Disclosures

- 2.6.1 Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.
- 2.6.2 When requests to disclose personal data are received by telephone it is the responsibility of the member of staff taking the call to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised and seek advice from the relevant line manager.
- 2.6.3 If a personal request is made for personal data to be disclosed it is again the responsibility of the member of staff to whom the request is made to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.
- 2.6.4 Personal data will not be used in newsletters, websites or other media without the consent of the data subject.
- 2.6.5 Routine consent issues will be incorporated into the CLIC Trust student data gathering sheets, to avoid the need for frequent, similar requests for consent being made.
- 2.6.6 Personal data will only be disclosed to Police Officers or other outside agencies if they are able to supply a relevant document which notifies of a specific, legitimate need to have access to specific personal data.
- 2.6.7 A record will be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

2.7 Subject Access Requests

- 2.7.1 If the CLIC Trust receives a written request from a data subject to see any or all personal data that the Trust holds about them this will be treated as a legitimate Subject Access Request and the Trust will respond within the recommended 40 day deadline. An invoice will be generated to cover these costs.
- 2.7.2 Informal requests to view or have copies of personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the Trust will comply with its duty to respond within the 40 day time limit.

2.7.3 This policy will be included in the Staff Handbook.

2.7.4 Data protection statements will be included on all forms that are used to collect personal data.

2.8. Confidentiality & Security

2.8.1 Personal data that is confidential must be preserved in compliance with the Data Protection Principles as defined in the Data Protection Act 1998.

2.8.2 Paper records will be managed so that access is restricted to those who need to use the information and stored in secure locations to prevent unauthorised access.

2.8.3 Computer systems will be designed and computer files created with adequate security levels to preserve confidentiality. Those who use the Academy's computer equipment will have access only to the data that is both necessary for the work they are doing and held for carrying out that work.

2.9 Ownership of Data

The CLIC Trust is responsible for the personal data that it holds. This responsibility extends to any data that is processed by a third party. The Trust will hold a record of all data files that it owns containing personal data, whether on paper or electronic media. Where required, the necessary information will be passed to the Chief Operations Office to facilitate the notification of the data to the Information Commissioner.

2.10 Training

All members of staff who work with personal data, and their line managers, will receive appropriate training in the area of Data Protection.

Appendix 1 – Definitions

- 1) **Data Subject** is defined as a “living” individual who is the subject of Personal Data.
- 2) **Personal Data** is defined in the Act as information identifying a living individual (“data subject”). The School may process a wide range of personal data of pupils, their parents or guardians, as part of their operation. To qualify as personal data, the data must be biographical in a significant sense, having the data subject as its focus and affecting the data subject’s privacy. Personal data includes facts, any expression of opinion about an individual and any indication of the intentions of anyone in respect of that individual. Examples of personal data are: names and addresses; bank details; academic, disciplinary, admissions and attendance records; references; and examination scripts and marks.
- 3) **Educational Record** is defined as information that comes from a teacher, other employee of the Local Authority or School, the pupil or their parents.
- 4) **Sensitive Personal Data** is defined in the Act as information in respect of racial or ethnic origin, political opinions, religious beliefs or "other beliefs of a similar nature", membership of a trade union, physical or mental health, sexual life, criminal convictions and alleged offences.
- 5) **Data Controller** is defined as a person or organisation that, individually or as a group, determines the purpose of holding data, and the manner of data processing.
- 6) **Data Processor** is defined as a person who processes data on behalf of the data controller, other than an employee of the data controller and the processing must be carried out under a contract that is made or evidenced in writing. The contract must contain obligations on the data processor to act in accordance with the instructions of the data controller.
- 7) **Processing** includes obtaining, holding, recording, adding, deleting, augmenting, disclosing, destroying, printing or otherwise using data.
- 8) **Designated Individuals** includes the following:
 - Chief Operations Officer deals with staffing matters (along with the HR Manager)
 - Headteacher and Deputy with responsibility for Pastoral Support deals with general student matters
 - Headteacher/Designated Safeguarding Person(s) deal with Child Protection matters

Appendix 2 – Subject Access Request Form

1	Are you making this request for information on your own behalf?		Yes	
	<i>If Yes, please go to part 2-7</i> <i>If No, please complete parts 8-11</i>		No	
2	If you are making this request for information on behalf of someone else, please state the nature of your relationship with that person.		Parent	
			Guardian	
			Legal Representative	
			Other (please specify below)	
3	If you are making this request for information on behalf of someone else please provide the following information about yourself below:			
<i>If the applicant is not the data subject (the person we hold information on), we will always correspond with the applicant unless otherwise specified.</i>				
4	Name			
5	Address			
	Postcode			
6	Contact Numbers	Mobile		
		Daytime		
		Evening		
7	Email Address			
		If you would prefer email contact please tick here		

Please complete the following section, providing information about the Data subject (the individual whose information is being requested)

8	Name(s) <i>Include previous names</i>		
9	Address		
	Postcode		
10	Contact Numbers	Mobile	
		Daytime	
		Evening	
11	Email Address		
		If you would prefer email contact please tick here	<input type="checkbox"/>
12	Date of Birth (<i>if under 18</i>)		
13	Please provide details of information you think we hold in the data subject's name. To qualify as personal data, the data must be biographical in a significant sense, having the data subject as its focus and affecting the data subject's privacy. In addition, information held in manual/paper files will only be personal data if the file is highly structured.		
	<p><i>Reference numbers and departments where known</i></p> <p><i>Further details or description of information required</i></p>		

Under the 1998 Data Protection Act we are entitled to charge a small administration fee of £10 for processing your application. Please enclose your cheque, made payable to The CLIC Trust, unless you have been advised that the fee is not required.

We also require copies of two documents for each person to prove his or her identity, one of which should include a photograph of the person. The documents could include a passport, driving licence or any other official document, including a utility bill but showing only the name and address of the person and the name of the company, not any billing details.

If you are applying on someone else's behalf please enclose certified proof of identity for both the data subject and yourself. Where you are acting as a legal representative or guardian of the data subject certified proof of this must also be given. If you prefer, you may provide proof with an original document by attending the School in person and bringing these documents with you.

Failure to provide these documents with your application may mean your request is refused.

After completing the application, please check to ensure that all the information you have provided is accurate and all required documents are enclosed. Sign below and return the application to:

***The Chief Operations Officer, The CLIC Trust, Chorlton Park Primary School,
Mauldeth Road West, Chorlton, Manchester, M21 7HH***

Signed: _____

Date: _____

The CLIC Trust is committed to the principles defined in the 1998 Data Protection Act. As such, information on this document will be used only for the purposes described above. We may, however, store the data in manual or electronic form, but only for as long as we are required to do so by law.

Enquiries:

Information about the school's Data Protection Policy is available from the Chief Operations Officer. General information about the Data Protection Act can be obtained from the Information Commissioner Information Line 0303 123 1113, or visit their website www.ico.gov.uk