Tauheedul Education Trust

This policy is in line with the Vision of the Trust

Nurturing Today's Young People, Inspiring Tomorrow's Leaders

DATA PROTECTION POLICY

Tauheedul
Education Trust

Document Control

This policy has been approved for operation within:	All Trust Establishments
Date of last review	November 2016
Date of next review	November 2017
Review period	1 Year
Policy status	Statutory
Owner	Tauheedul Education Trust
Version	3

Contents

1 Introduction

1.1 Everyone has rights with regard to how their personal information is handled. During the course of the Trust's activities it will collect, store and process personal information and recognises the need to treat it in an appropriate and lawful manner.

1.2 The types of information that the Trust may be required to handle include details of current, past and prospective employees, suppliers, pupils, parents and others that the Trust communicates with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how the Trust may use that information.

1.3 This policy sets out the Trust's requirements for data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

1.4 If the requirements of the Data Protection Act are not adhered to, it can lead to criminal prosecution of an individual and fines of up to £500,000 being issued to the Trust.

1.5 To support this policy, staff shall apply associated procedures and participate in associated training if requested to by the Trust.

1.6 If a member of staff considers that the policy has not been followed in respect of personal data about themselves or others, it should be raised with the Senior Leadership Team of the establishment.

1.7 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

2 Aims

2.1 To ensure the Trust fulfils its statutory responsibilities under the Data Protection Act.

2.2 To ensure effective security and protection is given to data that has been provided by individuals to the Trust which is required for the management and operation of Trust establishments.

2.3 To support the mission, vision and values of the Trust and its establishments.

3 Who is Responsible for the Policy?

3.1 The Trust has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory or Trust framework. The Trust has delegated day-to-day responsibility for operating the policy to the Trust Central Team, Local Governing Body and Head of each establishment.

3.2 The Local Governing Body and Senior Leadership Team at each establishment has a specific responsibility to ensure the fair application of this policy and all members of staff are responsible for supporting colleagues and ensuring its success.

4 Definition of Data Protection Terms

4.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

4.2 **Data subjects** for the purpose of this policy include all living individuals about whom the Trust holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

4.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address, date of birth or biometric) or it can be an opinion (such as a performance appraisal).

4.4 **Data controllers** are the people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. The Trust is the data controller of all personal data used in each of the establishments. The Trust is registered with the Information Commissioners Office (ICO Registration Z3350256) as the Data Controller. This registration covers all Trust establishments and their permitted use of data processing.

4.5 **Data co-ordinator** is the Head of Governance and Corporate Services who is the principal Trust contact for establishments with regard to implementation of the Data Protection Policy.

4.6 **Data champion** is the nominated lead within each Trust establishment to ensure implementation of the Data Protection Policy. The Head of Establishment shall ensure these persons are nominated and the role is reflected within their Job Description and their responsibility is known within the establishment.

4.7 **Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following the Trust's data protection and security policies at all times.

4.8 **Data processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on the Trust's behalf.

4.9 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

4.10 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

5 Data Protection Principles

5.1 Anyone processing personal data must comply with the eight enforceable Principles of Good Practice. These provide that personal data must be:

5.1.1 processed fairly and lawfully;

5.1.2 processed for limited purposes and in an appropriate way;

5.1.3 adequate, relevant and not excessive for the purpose;

5.1.4 accurate;

5.1.5 not kept longer than necessary for the purpose;

5.1.6 processed in line with data subjects' rights;

5.1.7 secure;

5.1.8 not transferred to people or organisations situated in countries without adequate protection.

5.2 In applying the Data Protection Act the Trust will also be aware of data protection exemptions. This will include exemptions from the requirement to:

5.2.1 grant subject access to personal data;

5.2.2 give privacy notices;

5.2.3 not disclose personal data to third parties.

6 Fair and Lawful Processing

6.1 The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case, the Trust), the purpose for which the data is to be processed by the Trust or its establishment, and the identities of anyone to whom the data may be disclosed or transferred.

6.2 For personal data to be processed lawfully, certain conditions have to be met. These include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In all cases, the data subject's explicit consent to the processing of such data will be required.

7 Processing for Limited Purposes

7.1 Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

8 Adequate, Relevant and Non-Excessive Processing

8.1 Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

9 Accurate Data

9.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

9.2 The Trust's Records Management Policy should be referred to for guidance on both the timescales for the checking of data and also for destruction of data.

10 Timely Processing

10.1 Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from systems when it is no longer required.

11 Processing in Line with Data Subjects' Rights

11.1 Data must be processed in line with data subjects' rights. Data subjects have a right to:

11.1.1 request access to any data held about them by a data controller;

11.1.2 prevent the processing of their data for direct-marketing purposes;

11.1.3 ask to have inaccurate data amended; and to

11.1.4 prevent processing that is likely to cause damage or distress to themselves or anyone else.

12 Data Security

12.1 The Trust will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

12.2 The Trust will have in place appropriate procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

12.3 In line with Trust Privacy Notices, we will not share information with third parties without consent unless the law allows us to.

12.4 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures, in line with the Data Protection Act, an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

12.5 Personal data will only be transferred to a third-party data processor if that party agrees to comply with Trust policies and procedures on data transfer, including electronic data transfer.

12.6 Third parties with whom we contract, who will be able to access data as part of that contract, will have to undergo a due diligence check as part of our procurement process. Third parties who do not meet acceptable standards of data security will not be contracted with. If the Trust becomes aware of any data security concerns regarding a third party with whom we contract, we will reserve the right to terminate the contract.

12.7 Third parties will only be able to access Trust ICT systems if they have accepted that they will comply with our ICT security policies and procedures.

12.8 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

12.8.1 *confidentiality* means that only people who are authorised to use the data can access it;

12.8.2 *integrity* means that personal data should be accurate and suitable for the purpose for which it is processed; and

12.8.3 *availability* means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the Trust's network instead of individual PCs or other devices.

12.9 Security procedures include:

12.9.1 entry controls: any stranger seen in entry-controlled areas should be reported.

12.9.2 secure lockable desks and cupboards: desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential).

12.9.3 methods of disposal: paper documents should be shredded and electronic data storage devices should be physically destroyed when they are no longer required.

12.9.4 equipment: data users should ensure that individual monitors do not show confidential information to passers-by and that they lock or log off from their PC when it is left unattended.

12.9.5 ICT: establishments shall ensure that ICT security policies and procedures are implemented.

13 Data Loss

13.1 All incidents relating to data loss or a near-miss with regards to data loss of both physical and ICT data must be reported to the Trust as Data Controller via the Data Co-ordinator at the Trust Central Office.

14 Dealing with Subject Access Requests

14.1 A formal request from a data subject for information that the Trust holds about them must be made in writing. A Trust Subject Access Request (SAR) Form has been developed to assist with the provision of information required to make a request - but it is not requirement for this form to be used.

14.2 A fee is payable by the data subject for provision of this information, the current level of fees are outlined on the SAR Form.

14.3 Any member of staff who receives a written request should forward it to their Head of Establishment immediately, who will then contact the Data Co-ordinator at the Trust Central Office for further guidance.

14.4 There are specific timescales for responding to a SAR. Therefore there shall be no delay in notification.

15 Providing Information over the Telephone

15.1 Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by the Trust. In particular they should:

15.1.1 verify the caller's identity to make sure that information is only given to a person who is entitled to it;

15.1.2 suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be verified; or

15.1.3 refer to the Senior Leadership Team for assistance in difficult situations - no-one should be bullied into disclosing personal information.

16 Monitoring, Evaluation and Review

16.1 The policy will be promoted and implemented throughout all Trust establishments.

16.2 The Trust will monitor the operation and effectiveness of arrangements referred to in this policy at each Trust establishment.

16.3 The Trust will review this policy every year in consultation with each Trust establishment.