DATA PROTECTION (ACADEMY/FREE SCHOOL) POLICY

Effective Date:	July 2016
Last Reviewed:	June 2015
Reviewed By:	Jon Wilson
Next Review Date:	June 2017
Version:	4

Data Protection Policy

1. Scope

This policy applies to all staff and students/learners of all The Shared Learning Trust Academies and Free Schools. The term data refers to all types of information records, not limited to electronic data.

2. Context

The Shared Learning Trust is committed to protecting the rights and privacy of its learners and staff in accordance with the Data Protection Act 1998.

The Trust needs to process certain information about its staff, learners and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to run courses, to record progress, to collect fees and to comply with legal obligations of funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely, and securely and not disclosed to any third party unlawfully.

The policy applies to all staff and students of the Trust. Any breach of the Data Protection Act 1998 or The Shared Learning Trust Data Protection Policy is considered to be an offence and in that event, disciplinary procedures may apply. As a matter of good practice, other parties and individuals working with the Trust, and who have access to personal information, will be expected to have read and comply with this policy.

3. Aims

The purpose of the Data Protection Act 1998 is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and wherever possible is processed with their consent.

4. Statutory position

Under the provisions of the Data Protection Act 1998, individuals have a right to know what personal is being held by The Shared Learning Trust and why it is being held. Data subjects may challenge the data if they find that they are wrong and may also seek redress through the Courts.

5. Policy Detail - Definitions

5.1 Personal Data

Data relating to a living individual who can be identified from that information. Includes name, address, telephone number, id number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

5.2 Sensitive Data

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, sexual orientation, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data is subject to much stricter conditions of processing.

5.3 Data Controller

Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data is collected and the way in which the personal data is processed.

5.4 Data Subject

Any living individual who is the subject of personal data held by an organisation.

5.5 Processing

Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data, accessing, altering, adding to, merging, deleting, retrieving, consultation or use of data disclosure, or otherwise making available of data.

5.6 Third Party

Any Individual/organisation other than the data subject, the data controller or its agents.

5.7 Relevant Filing System

Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

6. Responsibilities under the Data Protection Act 1998

For individual academies and schools, the Data Protection Officer is the Principal. Under ICO (Information Commissioners Office) guidance, individual academies no longer have to be registered separately under the data protection act.

The Trust is registered under number ZA121674, the Data Protection Officer for the central trust functions is the Trust Head of IT.

All staff in managerial roles are responsible for developing and encouraging good information handling practice within The Shared Learning Trust.

Compliance with data protection legislation is the responsibility of all members of The Shared Learning Trust who process personal information.

Members of The Shared Learning Trust are responsible for ensuring that any personal data supplied to The Shared Learning Trust are accurate and up-to-date.

7. Notification to the Information Commissioner

Notification is the responsibility of the Data Protection Officer.

Details of notification are published on the Information Commissioner's website.

Anyone who is, or intends, processing data for purposes not included within the notification should seek advice from the appropriate Data Protection Officer.

8. Data Protection Principals

All processing of personal data must be done in accordance with the eight data protection principles.

Principle 1: Personal data shall be processed fairly and lawfully. Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

Principle 2: Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes. Data obtained for specified purposes must not be used for a purpose that differs from those purposes.

Principle 3: Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held. Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.

Principle 4: Personal data shall be accurate and, where necessary, kept up to date. Data, which is kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate. It is the responsibility of individuals to ensure that data held by The Shared Learning Trust is accurate and up-to-date. Completion of an appropriate enrolment or application form etc. will be taken as an indication that the data contained therein is accurate. Individuals should notify The Shared Learning Trust of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of The Shared Learning Trust to ensure that any notification regarding change of circumstances is noted and acted upon.

Principle 5: Personal data shall be kept only for as long as necessary.

Principle 6: Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.

Principle 7: Personal Data shall be kept safe from unauthorised access, accidental loss or destruction. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

Principle 8: Personal data shall not be transferred to a country or a 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. Data must not be transferred outside of the European Economic Area (EEA) - the EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. Members of The Shared Learning Trust should be particularly aware of this when publishing information on the

Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

9. Data Subject Rights

Data Subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision making process that will significantly affect them.
- To prevent processing likely to cause damage or distress.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the Information Commissioner to assess whether any provision of the Data Protection Act has been contravened.

10. Consent

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The Shared Learning Trust understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. In most instances, consent to process personal and sensitive data is obtained routinely by The Shared Learning Trust (e.g. when a candidate signs an application form). Any forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data is to be published on the Internet as such data can be accessed from all over the world. Therefore, not gaining consent could contravene the eighth data protection principle. If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place. If any member of The Shared Learning Trust is in any doubt about these matters, they should consult the appropriate Data Protection Officer.

11. Data Security

All staff are responsible for ensuring that any personal data (on others) which they hold is kept securely and that it is not disclosed to any unauthorised third party. All personal data should be accessible only to those who need to use it. Staff should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- In a lockable room with controlled access, or
- In a locked drawer or filing cabinet, or
- If computerised, stored on network on not on PCs / Laptops which could be more easily stolen
- Never stored data on portable storage devices such as USB drives
- Not stored on Cloud based storage whether this be corporate or personal based. e.g. One Drive, Dropbox, Googledocs

Care should be taken to ensure that computer screens are not visible except to authorised staff and that computer passwords are kept confidential. Workstations must be locked when not in use. Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff and students/learners who process personal data "off-site". Offsite processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and students/learners should take particular care when processing personal data at home or in other locations outside The Shared Learning Trust main sites. Further guidance in this area is provided by the Acceptable Usage Policy (AUP)

12. Data Access Rights

Members of The Shared Learning Trust have the right to access any personal data which is held by The Shared Learning Trust in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by The Shared Learning Trust about that person.

Any individual who wishes to exercise this right should apply in writing to the Data Protection Officer. The Shared Learning Trust reserves the right to charge a fee for data subject access requests (currently £10). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee. In order to respond efficiently to subject access requests The Shared Learning Trust needs to have in place appropriate records management practices.

13. Data Disclosure

The Shared Learning Trust must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. Third party also includes other legal entities within The Shared Learning Trust. All staff and students/learners should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter.

The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of The Shared Learning Trust business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of

The Shared Learning Trust concerned. This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

The individual has given their consent (e.g. a student/member of staff has consented to The Shared Learning Trust corresponding with a named third party)

Where the disclosure is in the legitimate interests of the institution (e.g. disclosure to staff - personal information can be disclosed to other The Shared Learning Trust employees if it is clear that those members of staff require the information to enable them to perform their jobs): -

- Where the institution is legally obliged to disclose the data (e.g. government funding returns)
- Where disclosure of data is required for the performance of a contract (e.g. informing a student's LEA or sponsor of course changes/withdrawal etc.).
- The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:
  - To safeguard national security*
  - Prevention or detection of crime including the apprehension or prosecution of offenders*
  - Assessment or collection of tax duty*
  - Discharge of regulatory functions (includes health, safety and welfare of persons at work) *
  - To prevent serious harm to a third party
  - To protect the vital interests of the individual - this refers to life and death situations

* Requests must be supported by appropriate paperwork and confirmed identification of the source seeking the information.

When members of staff receive enquiries as to whether a named individual (e.g. a student) is a member of The Shared Learning Trust, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of The Shared Learning Trust may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request. As an alternative to disclosing personal data, The Shared Learning Trust may offer to do one of the following:

- Pass a message to the data subject asking them to contact the enquirer
- Accept a sealed envelope/incoming email message and attempt to forward it to the data subject

Please remember to inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of The Shared Learning Trust" to avoid confirming their membership of, their presence in or their absence from the institution.

Having received a request for personal data, the staff member must not make any special amendment or deletion to the data which would not otherwise have been made. The information must not be tampered with in order to make it acceptable to the Data Subject.

14. Subject Access Requests

Individuals wishing to access their personal information should submit a request in accordance with the following notes:

- Make your request in writing to the appropriate Data Protection Officer
- The request should include details and provide documented evidence of who you are (e.g. copies of driving licence, passport, birth certificate, student/Staff ID card). You should also provide as much detail as possible regarding the information you wish to access (e.g. where and by whom information is believed to be held, specific details of information required etc.).
- You are not required to state WHY you wish to access the information: the details we require are merely those that will aid the efficient location and retrieval of information.
- The Shared Learning Trust adopts a general policy of openness in terms of allowing individuals access to their personal information but reserves the right to charge a £10 administration fee.
- Once the Data Protection Officer receives a Subject Access Request, all efforts will be made to fully comply within 40 days. In any event, you will receive all the information that has been located and can be released within 40 days and an explanation for any information that cannot be provided at
  that time.
- In accordance with the Data Protection Act 1998, The Shared Learning Trust does not usually release information held about individuals without their consent. Therefore, if information held about you also contains information related to a third party, The Shared Learning Trust will make every effort to anonymise the information. If this is not possible, and The Shared Learning Trust has been unable to secure the relevant consent, The Shared Learning Trust may decide not to release the information.
- All queries should be directed to the appropriate Data Protection Officer in the first instance.

Any member of staff who receives a subject access request from a data subject must forward it immediately to the appropriate Data Protection Officer.

15. Retention and Disposal of Data

The Shared Learning Trust discourages the retention of personal data for longer than they are required.

16. Publication of The Shared Learning Trust Information

All members of The Shared Learning Trust should note that The Shared Learning Trust publishes a number of items that include personal data, and will continue to do so. These personal data are:

1. Personal data in marketing materials such as a prospectus (including photographs), alumni information, etc.

2. Staff data on The Shared Learning Trust website / intranet (including photographs). It is recognised that there might be occasions when a member of staff, a student, or a member of The Shared Learning Trust, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, The Shared Learning Trust should comply with the request and ensure that appropriate action is taken.

17. Direct Marketing

Any area that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes (e.g. an opt-out box on a form).

18. Roles and Responsibilities

18.1 The Board of Directors are responsible for ensuring that the Academy complies with legislation, and that this plan and any related procedures and action plans are implemented.

18.2 The appropriate Principal is responsible for implementing the policy, for ensuring that all staff are aware of their responsibilities, for providing them with appropriate training and support, and for taking appropriate action.

18.3 Day to day responsibility for co-ordinating and implementing this policy is with the Academy Principal.

18.4 All staff/others are expected to adhere to this policy as required by The Shared Learning Trust Code of Conduct.

19. Monitoring and Review

19.1 This policy will be reviewed every year.

19.2 Its outcomes will be assessed by monitoring Annual Development Plans (ADPs).

19.3 Its impact and effectiveness will be judged in terms of the positive benefits and any negative consequences arising from its implementation.

20. Dissemination

20.1 All policies that need to be conveyed to students/learners, staff and families will be available on The Shared Learning Trust website.

20.2 Staff will be informed about policies during induction and through on-going in-service training.