Trinity Multi Academy Trust

Policy:	Data Protection Policy
Date or review:	October 2016
Date of next review:	October 2018
Lead professional:	HR Director
Status:	Statutory

1. Purpose of policy and guiding principles

1.1 The Academy Trust has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

1.2 The Directors of the Trust have delegated a number of responsibilities to Governing Bodies within each Academy and the purpose of this document is to provide individual academy's with a policy, and procedures, that the Governing Body have adopted to make clear standards and expectations of all staff, in relation to using and protecting data.

1.3 The purpose of this policy is:

- to comply with statutory requirements, in respect of the 1998 Data Protection Act and any subsequent legislation, to ensure that personal data is treated in manner that is fair and lawful;
- to comply with information and guidance displayed on the Information Commissioners website (www.dataprotection.gov.uk);
- to comply with any relevant guidance and advice from relevant sources i.e. Diocese of Wakefield, Calderdale MBC.
- to ensure that all employees are aware of the academy expectations, in relation to using data and to make employees aware of the implications of abusing the intended use of data.
- to clarify the conditions under which data is stored and the purpose of retaining data
- to provide guidance to ensure that staff are protected from potential allegations of misuse, or misconduct.

1.4 Any enquiries about the Trust's academy's data protection policy, or related data storage or access matters should be directed to the Trust Data Controller in the first instance

2. Links with other policies or legislation

2.1. This policy is underpinned by the Data Protection Act 1998.

2.2. This policy links with the Use of Technology policy, assessment policies and practice, home/school agreements and the agreed publication scheme.

2.3. This policy forms part of the terms and conditions of employment for all staff.

3. Provisions

3.1. Key terms

"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.

"personal data" means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, internet or media.

"parent" has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

"the Act" refers to the Data Protection Act 1998.

3.2. Data gathering and processing

3.2.1. The Trust undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data is held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

3.2.2. All personal data relating to staff, students or other people with whom the Trust has contact, whether held on computer or in paper files, is covered by the Act.

3.2.3. Privacy notices will be issued to new students and staff, as required by the Data Protection Act. Privacy notices do not need to be sent to every individual therefore these details will be displayed in an appropriate way.

3.3. Data storage

3.3.1. Personal data will be stored in a secure and safe manner.

3.3.2. Electronic data will be protected by password procedures and firewall systems operated by the academy.

3.3.3. Workstations in shared working areas will be positioned so that they are not visible to casual observers waiting either in the office or outside the area.

3.3.4. Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.

3.3.5. Particular attention will be paid to the need for security of sensitive personal data.

3.3.6. General security measures, such as building security, storage of disks, printouts, confidential waste and physical files are in place across the academy.

3.3.7. Specific IT security systems are detailed in the IT policy and procedures.

3.3.8. Any queries about the security of data should be referred to the appropriate manager, or a member of SLG.

3.4. Data accuracy

3.4.1. Data will be as accurate and up to date as is reasonably possible. If a data subject informs the academy of a change of circumstances their records will be updated as soon as is practicable.

3.4.2. A print out will be issued to data subjects of their data record no less than every 12 months, so they can check its accuracy and make any amendments. Appendix 1 shows an example of the Data Collection form for students.

3.4.3. Routine consent and medical information will be incorporated into an academy's student data gathering sheets, to avoid the need for frequent, similar requests for consent being made throughout the year.

3.4.4. Any errors or changes will be rectified, and if the incorrect information has been disclosed to a third party, any recipients will be informed of the correct data.

3.4.5. In cases where this informal resolution is not sufficient and a data subject challenges the accuracy of their data the academy will mark the record as 'challenged'. If informal resolution is not possible, the dispute will be referred to the Governing Body for their judgement. If the dispute cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

3.5. Data adequacy and relevance

3.5.1. Data held about people will be adequate, relevant and not excessive in relation to the purpose for which it is being held.

3.5.2. To comply with this, the academy will check records regularly for missing, irrelevant or potentially excessive data that is being held. In these cases the academy may contact the data subject to verify the data held.

3.5.3. Checks will be the responsibility of the HR Director for staff records and a Vice Principal for student records. These members of SLG will delegate these tasks as

appropriate. The decision on what should be deleted will be with each of these members of SLG.

3.5.4. Data held about individuals will not be kept longer than necessary for the purposes registered. The SLG staff named above are responsible for ensuring obsolete data is properly erased.

3.6. Dismissal, grievance and dismissal

3.6.1. Employees have the same rights of access to files containing information about disciplinary matters or grievances about themselves as they do to other personal data held, unless this information is associated with a criminal investigation, in which case an exemption might apply. All of the normal data protection and access obligations apply to data created or accessed in the course of dealing with disciplinary and grievance issues. Any information referring to a third party must be removed or anonymised before access is granted.

3.6.2. Disciplinary warnings typically 'expire' (as defined by the staff disciplinary policy), provided that no further warnings have been issued and no disciplinary action has been taken against the employee during that period. In these circumstances, the warnings will generally be disregarded for future disciplinary purposes but not removed from the personal file. There may be occasions, however, for example in the case of gross misconduct, or gross negligence, where the nature of the offence does not make it desirable and practicable for the time limit to apply. If this is so, the employee must be notified in writing when the warning is given of the period applicable, which will not normally exceed 5 years. Exceptions to the time limit will apply where child protection issues are raised.

4. Data disclosures

4.1. Any personal data will, in general, only be disclosed to organisations or individuals for whom consent has been given to receive the data.

4.2. There are circumstances under which the Trust, or an academy within the Trust, may need to disclose data without explicit consent for that occasion. These circumstances are:

- student data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- student data disclosed to authorised recipients in respect of their child's health, safety and welfare
- student data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school.
- only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the academy by staff will only be made available where the person requesting the information is a professional legitimately working within the academy who **need to know** the information in order to do their work. The academy will not disclose anything on students' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

4.3. To summarise, a **"legal disclosure"** is the release of personal information from a computer to someone who requires the information to do his or her job within or for the Trust, provided that the purpose of that information has been registered. An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the Trust's registered purposes.

4.4. When requests to disclose personal data are received by telephone it is the responsibility of the member of staff receiving the request 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. Failure to not undertake some level of check could be considered misconduct, depending on the nature of the data request.

4.5. If a personal request is made for personal data to be disclosed it is again the responsibility of the member of staff receiving the request 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.

4.6. Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

4.7. Requests from staff, students, or parents for personal, or friendly reasons, should be politely refused. For example, the address or birth date of a colleague, the address of a classmate, or class lists for reasons such as get well cards, birthday greetings etc. In line with the Act permission would need to be sought from the data subject(s). Advice should be sought from the HR Director for staff records and the Vice Principal for student records. These members of SLG will make the decision on how to proceed.

4.8. Personal data will only be disclosed to Police Officers if they are able to supply a WA170 form which notifies of a specific, legitimate need to have access to specific personal data.

4.9. A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

5. Subject Access Requests

5.1. The Act extends to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place.

5.2. Formal requests for access must be writing.

5.3. The data subject should ask for a Data Subject Access form (Appendix 2). These are available from the Executive Principal's PA, completed forms should be returned to Executive Principal's PA (the nominated officer). Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (eg Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

5.4. If a written request is received from a data subject to see any or all personal data that the Trust holds about them this should be treated as a Subject Access Request and this will be responded to within the 40 day deadline.

5.5. Informal requests to view or have copies or 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 this will be treated as a formal request.

5.6. If a written request from a parent regarding their own child's record is received, access to the record will be provided within 15 school dates in accordance with the current Education (Pupil Information) Regulations.

5.7. Where a request for subject access is received in relation to a reference (either provided or requested for an applicant), please refer to (Appendix 3).

5.8. Where a request for subject access is received from a student, the policy is:

- Requests from students will be processed as any subject access request as outlined below and the copy will be given directly to the student, unless it is clear that they do not understand the nature of the request.
- Requests from students who do not appear to understand the nature of the request will be referred to their parents.

- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

6. Roles and responsibilities

6.1. The role of the Executive Principal/Principal

6.1.1. The role of Principal is to ensure that this policy is applied fairly and consistently across the academy.

6.1.2. The Principal, will delegate to appropriate members of staff responsibilities within this policy, including informing all staff of the policy which has been adopted.

6.2. The role of the Directors and Governing Body's

6.2.1. The Directors will approve this policy for a Governing Body to adopt.

6.2.2. The Governing Body will monitor, evaluate and review policies in line with statutory and best practice guidelines.

6.3. The role of SLG

6.3.1. The HR Director is responsible for the gathering and storage of staff personal data.

6.3.2. The nominated Vice Principal is responsible for the gathering and storage of student personal data

6.4. The role of the employee/other staff

6.4.1. The Network Manager is responsible for ensuring this policy is covered in the IT induction, and the computer storage of data.

6.4.2. The Administration Manager is responsible for the paper records held by an academy.

6.4.3. All employees should:

- be committed to the principals of this policy
- be aware of their own responsibilities
- refer any queries to their line manager, or a member of SLG.

7. Monitoring and Evaluation

7.1. Data protection statements will be included in academy prospectus' and on any forms that are used to collect personal data.

7.2. All data requests will be recorded in the Subject Access log book.

7.3. Any concerns will be brought to the Principal in the first instance.

7.4. This policy should be reviewed at least every two years to ensure compliance to legislation, academy needs and good practice.

7.5. This policy will be promoted and implemented throughout the academy and will be included in the IT induction for all new staff.

7.6. The Act specifically allows for processing of data on racial or ethnic origin, religion and disability if it is necessary for keeping under review the existence, or absence, of equality of opportunity. The collection of this information is exclusively used for the statistical evaluation as defined by the Equalities Act 2010. The academy, where possible, will ensure anonymity of information when meaningful monitoring is required.

Appendix 1 – Example of data collection sheet

Trinity Academy Halifax
Data Collection Sheet

Please complete the information below and return to the academy office

Legal Surname:	**Preferred Surname:**
Legal Forename:	
Middle Name:	**Preferred Forename:**
Date of Birth:	
Address:	**Year:**
Post Code:	
Telephone:	

Please give details of **all** persons who have **parental responsibility** and anyone else you wish to be contacted in an emergency.
Place them in the order that you wish for them to be contacted in an emergency,

Priority	Name and Relationship	Does this person have parental responsibility?	Home address/telephone number/mobile	Work telephone number
1	**Name:** **Relationship:**		**Address:** **Tel:** **Mobile:** **Email:**	 **Tel:**
2	**Name:** **Relationship:**		**Address:** **Tel:** **Mobile:** **Email:**	 **Tel:**

Meal arrangement
Please tick below the type of meal your child would normally have:
School meal ☐ Packed lunch ☐ Free meal ☐

Mode of travel to/from the academy
Please tick below the most frequently used method of travel:
Bicycle ☐ Car/Van ☐ Walk ☐ Taxi ☐ School bus ☐ Public bus service ☐

Name of medical practice:

Telephone number:

Medical condition(s)/information:

Student assessed as disabled: Yes / No *(please circle as appropriate)*

Ethnicity (eg Pakistani/White British):
Religion:
Home language: **First language:**

Armed Forces information:
Does either parent serve in the armed forces, for example the Navy, Army etc? Yes / No *(please circle as appropriate)*
If yes, which one? _____

Photographs: Photographs of events, activities and the participants will be taken at various times throughout the year. You can choose to give your consent or not. All imagery will be taken and used responsibly.
If you **DO NOT** wish to give consent, please tick here:

Data Protection Act 1998: The academy is registered under the Data Protection Act for holding personal data. The academy has a duty to protect this information and to keep it up to date. The academy is required to share some of the data with the Local Authority and with the DE.

Signature: **Date:**

Appendix 2 - Data Subject Access Request Form

Trinity Multi Academy Trust

Data Protection Act 1998 – Data Subject Access request form

Under section 7 of the Data Protection Act 1998, an individual is entitled to ask for information the Academy holds about her/him. This entitlement is known as the "Right of Access to Personal Data."

In exercise of the rights granted to me under the Data Protection Act 1998, I request that the academy provides me with details of the personal data it holds about me and the purposes for which it is used.

I am aware that, under section 7.3 of Data Protection Act 1998, the academy is not obliged to comply with my request unless they are supplied with such information as they may reasonably require in order to satisfy themselves as to my identity and to locate the information which I seek.

DATA SUBJECT (please use BLOCK CAPITALS)			
Full Name		Date of birth	
Address		Telephone Number	
Post code		Length of time at this address	(yrs/months)
Previous address(es) with dates (if data is required for this period)			

Declaration – please complete section (a) and either section (b) or (c)

Section (a) (please tick)
I am providing proof of identity through:

- ❑ my driving licence
- ❑ passport
- ❑ birth or marriage certificate
- ❑ benefit book

and confirmation of my current permanent home address is provided through:

- ❑ the same document
- ❑ a current utility bill in the same name as my birth/marriage certificate

And either section (b) I confirm that I am the Data Subject.

Signed…….…… Date……..

Or section (c) I confirm that that I am acting on behalf of the data subject and have submitted proof of my authority to do so.

Signed…….. Date…….....…….

Full Name		Date of birth	
Address		Telephone Number	
Post code			

INFORMATION REQUESTED

Please complete the section below to enable the Trust to locate the information that you require. If you would like to provide us with other information on the data you are seeking, please use the space below. If you want information that relates to a specific time period or experience, the details would help us to focus our search and respond more quickly.

Please use BLOCK CAPITALS, provide as much detail as possible and continue on separate sheet if necessary.

Please return completed form with proof of identity and address to the Executive Principal's PA

Appendix 3

Subject access and employment references – Good Practice

This good practice note clarifies how the Data Protection Act 1998 applies to employment references. The recommendations also apply to other types of reference, such as those provided for educational purposes.

The main issues
The Information Commissioner receives a lot of enquiries about:

- whether organisations can release a reference to the person who is the subject of the reference
- how the Act applies to references; and
- the fact that references may have been given 'in confidence'.

Individuals have a right to a copy of information held about them that is covered by the Act. When an individual asks for a copy of a reference written about them, many employers refuse to provide it because it was supplied in confidence. This may breach the Act. The Act applies differently to references which have been given by an employer and those which have been received by an employer.

Do you have to give a copy of a reference you have written?
If someone asks for a copy of a confidential reference you have written about them relating to training, employment or providing a service, you do not have to provide it because of an exemption in the Act. However, you may choose to provide the information. It would seem reasonable to provide a copy if a reference is wholly or largely factual in nature, or if the individual is aware of an appraisal of their work or ability.

Do you have to give a copy of a reference you have received from someone else?
References received from another person or organisation are not treated in the same way. If you hold the reference in a way that means it is covered by the Act, you must consider a request for a copy under the normal rules of access. An individual can have access to information which is about them, but may not necessarily have access to information about other people, including their opinion, provided in confidence.

The references you have received may be marked 'in confidence'. If so, you will need to consider whether the information is actually confidential. You cannot sensibly withhold information which is already known to the individual. Factual information such as employment dates and absence records will be known to an individual and should be provided. Information relating to performance may well have been discussed with the employee as part of an appraisal system. Where it is not clear whether information, including the referee's opinions, is known to the individual, you should contact the referee and ask whether they object to this being provided and why.

Even if a referee says that they do not want you to release their comments, you will need to provide the reference if it is reasonable in all the circumstances to comply with the request without their consent. You should weigh the referee's interest in having their comments treated confidentially against the individual's interest in seeing what has been said about them. When considering whether it is reasonable in all the circumstances to comply with a request, you should take account of factors such as:

- any express assurance of confidentiality given to the referee
- any relevant reasons the referee gives for withholding consent
- the potential or actual effect of the reference on the individual
- the fact that a reference must be truthful and accurate and that without access to it the individual is not in a position to challenge its accuracy

- that good employment practice suggests that an employee should have already been advised of any weaknesses
- and any risk to the referee.

You should consider whether it is possible to keep the identity of the referee secret.

Recommended good practice

In most circumstances, you should provide the information in a reference, or at least a substantial part of it, to the person it is about if they ask for it. Even if the referee refuses consent, this will not necessarily justify withholding the information, particularly where this has had a significant impact on the individual, such as preventing them from taking up a provisional job offer.

However, there may be circumstances where it would not be appropriate for you to release a reference, such as where there is a realistic threat of violence or intimidation by the individual towards the referee. You should consider whether it is possible to conceal the identity of the referee, although often an individual will have a good idea who has written the reference.

If it is not reasonable in all of the circumstances to provide the information without the referee's consent, you should consider whether you can respond helpfully anyway (for example, by providing a summary of the content of the reference). This may protect the identity of the referee, while providing the individual with an overview of what the reference says about them.