Data Protection Policy

Review by Trustees:	**March 2016**
Adopted by Governing body of	
Date/Minute Ref:	
Next Full Review Due:	**September 2018**
Reviewer:	**Director of Operations**

Huddersfield Horizon SCITT
Data Protection Policy
2016-2018

General Statement
The Board of Trustees provides extensive guidance and is responsible for monitoring statutory compliance on behalf of the Trust and is responsible for monitoring statutory compliance in relation to the information provided to the regulators, parents and others. The Local Governing Body has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Principal and Governors of this Academy intend to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1988. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines. Staff are trained and updated regularly.

Enquiries
Information about the academy's Data Protection Policy is available from *the SCITT director*. General information about the Data Protection Act can be obtained from the Data Protection Commissioner (Information Line 01625 545 745, website www. dataprotection.gov.uk).

Fair Obtaining and Processing *The Huddersfield Horizon SCITT* 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 are 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.

• **"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.

Registered Purposes
The Data Protection Registration entries for the Academy are available for inspection, by appointment, at the academy office. Explanation of any codes and categories entered is available from the *SCITT director* who is the person nominated to deal with Data protection issues in the Academy. Registered purposes covering the data held at the academy are listed on the academy's Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

Data Integrity
The academy undertakes to ensure data integrity by the following methods;

Data Accuracy
Data held 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 computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the Academy will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Board of Trustees for their judgement. If the problem 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.

Data Adequacy and Relevance
Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the Academy will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. A printout of their data record will be provided to data subjects every twelve months so that its adequacy and relevance can be checked and agreed by the academy and any amendments made.

Length of Time
Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Principal to ensure that obsolete data are properly erased.

Subject Access
The Data Protection Acts extend 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. Where a request for subject access is received from a student, the academy's policy is that:

♦ 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 the student does 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 or carers.

♦ 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.

Processing Subject Access Requests
Requests for access must be made in writing. Students parents or staff may ask for a Data Subject Access form, available from the Academy Office. Completed forms should be submitted to the . 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 subjects name, the name

and address of the requester (if different), the type of data required (e.g. student record, HR 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 the date on which sufficient information has been provided.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 academy day in accordance with the current Education (Student Information) Regulations.

Authorised Disclosures
The Academy will, in general, only disclose data about individuals with their consent. However there are circumstances under which the Academy's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:
♦ Student data disclosed to authorised recipients related to education and administration necessary for the academy 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 academy.

♦ 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 academy.

♦ Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the academy by business support staff, teachers and student support will only be made available where the person requesting the information is a professional legitimately working within the academy who **needs 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.
A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the academy, 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 Academy's registered purposes.

Data and Computer Security
The Huddersfield Horizon SCITT undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

Physical Security
Appropriate building security measures are in place, such as alarms, window bars, deadlocks, CCTV and computer hardware cable locks. Only authorised persons are allowed in the server room. Disks, tapes and printouts are locked away securely when not in use. Visitors to the

academy are required to sign in and out, to wear identification badges whilst in the academy and are, where appropriate, accompanied.

Logical Security
Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly.

Procedural Security
In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Overall security policy for data is determined by The Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. The Academy's security policy is kept in a safe place at all times.

Any queries or concerns about security of data in the academy should in the first instance be referred to the Principal.

Individual members of staff can be personally liable in law under the terms of the Data Protection Act. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

Further details on any aspect of this policy and its implementation can be obtained from: The Huddersfield Horizon SCITT Director.

J Acklam
Reviewed: June 2017 (R Batley)
Next review: September 2018

Appendix 1

Data protection principles

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or 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.

Appendix 2

Insert Academy Name

Subject access request

Name : .....

Address: .....

.....

Post code: .....

Status: Student / Staff / Parent

If parent or student
Name(s): of students on role: .....

DOB of student: .....

Please supply the information about me I am entitled to under the Data Protection Act 1998 relating to: (please list, where appropriate please include dates, and if CCTV locations, dates and times)

(Continue overleaf if required)

If you need any more information from me, or a fee, please let me know as soon as possible.

Signature: ..... *Date: .....*

This form should be placed in a sealed envelope,

addressed to insert name and role