



**ST HILDA'S**  
CATHOLIC ACADEMY TRUST

# **ST. HILDA'S CATHOLIC ACADEMY TRUST**

## **DATA PROTECTION POLICY**

**Policy Reviewed and Adopted by the Executive Board**

**Version 1.0**

**Date of Next Review: February 2019**

**Responsible Officer: DFCS**

## **General Statement**

1. The Directors of St. Hilda's Catholic Academy Trust (the 'Trust') have overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.
2. Directors of this Trust, Head Teachers and the Director of Finance & Corporate Services (DFCS) intend to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1998. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

## **Enquiries**

3. Information about the Trust's Data Protection Policy is available from the DFCS. General information about the Data Protection Act can be obtained from the Information Commissioner (Information Line - 01625 524510, website [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk); email: [mail@ico.qsi.gov.uk](mailto:mail@ico.qsi.gov.uk)).

## **Fair Obtaining and Processing**

4. 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.

"processing" means obtaining, recording or holding the information or data or carrying out any 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 any other 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**

5. The Data Protection Registration entries for the Trust are available for inspection, by appointment, with the DFCS. Explanation of any codes and categories entered is available from the DFCS who is the person nominated to deal with Data protection issues in the Trust and is the registered Data Protection Officer. Registered purposes covering the data held at the Trust are listed on the Trust'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**

6. The Trust undertakes to ensure data integrity by the following methods:

### ***Data Accuracy***

7. Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the Trust of a change of circumstances their computer record will be updated as soon as is practicable.
8. Where a data subject challenges the accuracy of their data, the Trust 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 Directors 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***

9. 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 Trust will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

### ***Length of Time***

10. Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Data Protection Officer to ensure academies are provided with relevant guidance in this area to ensure that obsolete data is properly erased.

### ***Subject Access***

11. 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 or on behalf of a pupil, the Trust's policy is that:
  - Requests from pupils will be processed as any subject access request as outlined below, and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
  - Requests from pupils 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***

12. Requests for access must be made in writing. Pupils, parents or staff may ask for a Data Subject Access form (See Appendix A), available from each academy's respective Business Manager.
13. Completed forms should be submitted to the Head Teacher, School Business Manager or DFCS. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access Log which will be maintained by each academy and the Central Trust Team.

14. Each Subject Access Log will contain the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date).
15. 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 working days in accordance with the current Education (Pupil Information) Regulations.*

### **Authorised Disclosures**

16. The Trust will, in general, only disclose data about individuals with their consent. However there are circumstances under which the authorised officers may need to disclose data without explicit consent for that occasion. These circumstances are strictly limited to:
  - Pupil data disclosed to authorised recipients related to education and administration necessary for the Trust to perform its statutory duties and obligations.
  - Pupil data disclosed to authorised recipients in respect of a child's health, safety and welfare.
  - Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the Trust.
  - 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 Trust. Officers and IT personnel working on behalf of the Trust are contractually bound not to disclose personal data.
  - Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the Trust by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the Trust who needs to know the information in order to do their work. The Trust will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything which suggests that they are, or have been, either the subject of or at risk of child abuse.
17. A "legal disclosure" is the release of personal information 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.
18. 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.

## **Data and Computer Security**

19. The Trust undertakes to ensure security of personal data by the following general methods:

### ***Physical Security***

20. Appropriate building security measures are in place. Passwords are used to access IT networks. Visitors to the Trust are required to sign in and out, to wear identification badges whilst on trust premises and are, where appropriate, accompanied.

### ***Logical Security***

21. 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. Back-up tapes must not be taken from the Trust's premises.

### ***Procedural Security***

22. 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.

23. Any queries or concerns about security of data in the Trust should, in the first instance, be referred to the respective Head Teacher, School Business Manager of DFCS.

24. Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. 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 DFCS at:

[farquhar.j@trinitycatholiccollege.org.uk](mailto:farquhar.j@trinitycatholiccollege.org.uk)

**Appendix A – DATA SUBJECT ACCESS FORM**

**ACCESS TO PERSONAL DATA REQUEST DATA PROTECTION ACT 1998 Section 7.**

Enquirer's Surname.....

Enquirer's Forenames.....

Enquirer's Address .....

.....

.....

.....

Enquirer's Postcode .....

Telephone Number .....

Are you the person who is the subject of the records you are enquiring about YES / NO (i.e. the "Data Subject")?

If NO,

Do you have parental responsibility for a child who is the "Data Subject" of the YES / NO records you are enquiring about?

If YES,

Name of child or children about whose personal data records you are enquiring

.....

Description of Concern / Area of Concern

.....

Description of Information or Topic(s) Requested (In your own words)

.....

Additional information.

.....

**N.B. Information will be supplied within 15 working days.**

Please dispatch Reply to: (if different from enquirer's details as stated on this form)

Name .....

Address .....

.....

Postcode .....

**DATA SUBJECT DECLARATION**

I request that the Trust search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the Trust.

I agree that the reply period will commence when I have supplied sufficient information to enable the Trust to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent)

.....

Name of "Data Subject" (or Subject's Parent)

(PRINTED).....

Dated .....