The Wythenshawe Catholic Academy Trust

# Data Protection Policy

St Paul's Catholic High School
St Elizabeth's Catholic Primary School
St Anthony's Catholic Primary School
SS John Fisher and Thomas More Catholic Primary School

| Document Record | |
|---|---|
| Title | Data Protection Policy |
| Date | February 2016 |
| Supersedes | N/A |
| Purpose | To ensure that all schools within the Trust comply with the Data Protection Act 1998. |
| Author | Wythenshawe Catholic Academy Trust |
| Review | March 2018 |
| Date considered by WCAT | February 2016 |
| Date consulted with unions | N/A |
| Date adopted by WCAT | March 2016 |
| Date distributed | March 2016 |

Schools within the Wythenshawe Catholic Academy Trust:

- St Paul's Catholic High School
- St Anthony's Catholic Primary School
- St John Fisher and St Thomas More Catholic Primary School
- St Elizabeth's Catholic Primary School

This policy will be published on the school's website and will be referred to in the school's brochure.

## Contents

1. **Introduction**

   i. The Wythenshawe Catholic Academy Trust (referred to hereafter as the Trust) is committed to all aspects of data protection and takes seriously its duties, and the duties of its employees, under the Data Protection Act 1998. This policy sets out how the Trust deals with personal data, including data subject access requests, and employees' obligations in relation to personal data.

   ii. The Trust collects and uses certain types of personal information about employees, students, parents and other individuals who come into contact with each school in the Trust in order to provide education and associated functions. In addition, the Trust may be required by law to collect and use certain types of information to comply with statutory obligations of Local (Education) Authorities (LAs), government agencies and other bodies.

2. **Scope of the policy**

   i. This policy applies to all schools within the Trust, currently consisting of St Paul's Catholic High School, St Anthony's Catholic Primary School, St John Fisher and St Thomas More Catholic Primary School and St Elizabeth's Catholic Primary School.

   ii. This policy applies to paid staff, volunteers and individuals engaged to work at the schools in an official capacity.

3. **Roles and responsibilities**

   i. The Wythenshawe Catholic Academy Trust is a legal entity and is registered with the Information Commissioner's Office (ICO) as the data controller under the 1998 Act. The Trust is therefore ultimately responsible for the data protection policy and any data breaches by the schools in the trust.

   ii. The Trust has delegated day to day matters regarding data protection to be dealt with by Headteachers, the Deputy Headteachers, the School Business Managers, the Strategic Resource Officer and the Strategic Finance Officer.

   iii. The Trust has identified Mrs Marion Fletcher as the data protection officer to be responsible for the implementation of this policy. If employees have any questions about data protection in general, this policy or their obligations under it, they should direct them to Mrs Marion Fletcher, contactable on 0161 437 3029.

   iv. The Trust will provide training to all employees on data protection matters on induction and on a regular basis thereafter. If an employee considers that he/she would benefit from refresher training, he/she should contact Mrs Marion Fletcher.

4. **Data protection principles**

   i. The Data Protection Act 1998 requires that eight data protection principles be followed in the handling of personal data. These principles require that personal data must:

      - be fairly and lawfully processed;
      - be processed for limited purposes and not in any manner incompatible with those purposes;
      - be adequate, relevant and not excessive;
      - be accurate;
      - not be kept longer than is necessary;
      - be processed in accordance with individuals' rights;
      - be secure; and
      - not be transferred to countries without adequate protection.

5. **"Personal data"**

   i. The Data Protection Act 1998 applies only to information that constitutes "personal data". Information is "personal data" if it:

      - identifies a person, whether by itself, or together with other information in the organisation's possession, or is likely to come into its possession; and
      - is about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature.

   ii. Consequently, automated and computerised personal information about employees and students is covered by the Act.

   iii. Personal data can include any expression of opinion about an individual and intentions towards an individual. In certain circumstances the Act may apply to personal data held visually in photographs and video clips (including CCTV) and as sound recordings.

   iv. Personal information stored physically (for example, on paper) and held in any "relevant filing system" is also covered. In addition, information recorded with the intention that it will be stored in a relevant filing system or held on computer is covered.

   v. A "relevant filing system" means a well-structured manual system that amounts to more than a bundle of documents about each individual filed in date order, ie a system to guide a searcher to where specific information about a named individual can be located easily.

6. **The use of personal information**

   i. The Data Protection Act 1998 applies to personal information that is "processed". This includes obtaining personal information, retaining and using it, allowing it to be accessed, disclosing it and, finally, disposing of it.

7. **"Sensitive personal data"**

   i. "Sensitive personal data" is information about an individual's:

   - racial or ethnic origin;
   - political opinions;
   - religious beliefs or other beliefs of a similar nature;
   - trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
   - physical or mental health or condition;
   - sex life;
   - commission or alleged commission of any criminal offence; and
   - proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

   ii. The Trust will process sensitive personal data, including sickness and injury records and references, in accordance with the eight data protection principles. If the Trust enters into discussions about a merger within the Trust or acquisition with a third party, the Trust will seek to protect employees' data in accordance with the data protection principles.

   iii. The Trust will not generally retain sensitive personal data without the express consent of the employee or the parent or guardian of the student in question.

8. **Personnel files and student records**

   i. An employee's personnel file is likely to contain information about his/her work history with the Trust and may, for example, include information about any disciplinary or grievance procedures, warnings, absence records, appraisal or performance information and personal information about the employee including address details and national insurance number.

   ii. There may also be other information about the employee located within the Trust, for example in his/her line manager's inbox or desktop; with payroll; or within documents stored in a relevant filing system.

   iii. The Trust may collect relevant sensitive personal information from employees for equal opportunities monitoring purposes. Where such information is collected, the Trust will anonymise it unless the purpose to which the information is put requires the full use of the individual's personal information. If the information is to be used, the Trust will inform employees on any monitoring questionnaire of the use to which the data will be put, the individuals or posts within the Trust who will have access to that information and the security measures that the Trust will put in place to ensure that there is no unauthorised access to it.

   iv. Student records will include each school to state the information that is collected and stored

9. **Security**

i. The Trust will ensure that 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.

ii. The Trust will ensure that personal information about an individual is securely retained. The Trust will keep hard copies of information in a locked filing cabinet. Information stored electronically will be subject to access controls and passwords and encryption software will be used where necessary.

iii. Where laptops and other electronic devices including removable media storage such as USB pens are taken off site, employees must follow the Trust's relevant policies relating to the security of information and the use of computers for working at home and bringing your own device to work.

iv. The Trust provides training on data protection issues to all employees who handle personal information in the course of their duties at work. The Trust will continue to provide such employees with refresher training on a regular basis. Such employees are also required to have confidentiality clauses in their contracts of employment.

**10. Retention of data**

i. The Trust will apply the records management policies and procedures to ensure that information is not held longer than is necessary.

ii. The Trust has a duty to retain some employee and student data for a period of time following their departure from their school, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time.

11. **Fair processing notice**

i. The Trust is committed to ensuring that individuals are aware that their data is being processed and:

- the types of information that it keeps about him/her;
- the purpose for which it is used; and
- the types of organisation that it may be passed to, unless this is self evident (for example, it may be self evident that an employee's national insurance number is given to HM Revenue & Customs and state here if student's exam results are published or given to external bodies.

ii. The Trust does not issue a standard privacy notice, the use for certain information is printed on the appropriate collection form or outlined in the school prospectus, information pack or on the schools website.

## 12. Data subject access requests

i. An employee has the right to access information kept about him/her by the Trust, including personnel files, sickness records, disciplinary or training records, appraisal or performance review notes, emails in which the employee is the focus of the email and documents that are about the employee.

ii. A student (normally age 12 or above) and dependent upon their maturity and capacity to understand, may also have the right to access information held about him/her by the Trust. The Headteacher will discuss the request with the student and take their views into account when making a decision. A student with the competency to understand can refuse consent to the request for their records being disclosed to their parent or guardian. The information held may include their each school to state if they hold their behaviour records, review notes, e-mails in which the student is the focus of the e-mail and documents that are about the student.

iii. Mrs Marion Fletcher is responsible for dealing with data subject access requests.

iv. The Trust will charge up to £10 for allowing individuals access to information about them. The Trust will respond to any data subject access request within **40 calendar days.**

v. The Trust will allow the individual access to hard copies of any personal information. However, if this involves a disproportionate effort on the part of the Trust, the employee shall be invited to view the information on-screen or inspect the original documentation at a place and time to be agreed by the Trust.

vi. The Trust may reserve its right to withhold an individual's right to access data where any statutory exemptions apply.

vii. An individual who wishes to exercise their right to access data should make a request in writing and submit it to the Headteacher. The school will ask to see evidence of their identity, such as their passport or driving licence, and proof of their entitlement to see such data before disclosure of any information.

## 13. Education (Pupil Information) (England) Regulations 2005

i. There are two distinct rights of access to information held by schools about students. There is also the right of those entitled to have access to curricular and educational records as defined within the Education (Pupil Information) (England) Regulations 2005. The difference between the Data Protection Act and the Pupil Information Regulations is that under the Pupil Information Regulations, parents of pupils in schools maintained by the Local Authority have a right to access their child's data and the child cannot prevent this. These regulations only cover information in the official pupil record.

ii. Under these regulations, the governing body of a school must make a pupil's educational record available for inspection by the parent, free of charge, within 15 school days of the parent's written request for access to that record. The school must also provide a copy of the record if requested to do so within 15 school days.

iii. There is no legal equivalent right to access a student's educational record if the child attends an English academy, a free school or an independent school. The Trust has consider each case on its own merit.

iv. The Education (Independent School Standards) Regulations 2014 (part 6 f) differ slightly to the above. Under these Regulations, academies must provide an annual written report of each registered pupil's progress and attainment in the main subject areas taught, to the parents of that registered pupil (except that no report need be provided where the parent has agreed otherwise).

v. The meaning of a parent is wider than the definition of who has parental responsibility. Parent means a person with parental responsibility or who has care of a child. Therefore, where a child is living with grandparents, the grandparents have a right to see the child's educational records even though they may not have parental responsibility. Information and guidance regarding parental responsibility can be found on the website www.gov.uk and the definition of a parent is defined in Section 576 of the Education Act 1996.

vi. The Trust will not communicate anything to a parent which it could not communicate to the student him/herself under the Act.

14. **Correction, updating and deletion of data**

i. The Trust has a system in place that enables employees to check their personal information on a regular basis so that they can correct, delete or update any data. If an employee becomes aware that the Trust holds any inaccurate, irrelevant or out-of-date information about him/her, he/she must notify their line manager immediately and provide any necessary corrections or updates to the information.

ii. The Trust has a system in place that enables information held on students to be checked each school to state how often your student information is sent out for checking i.e. annually so that they can correct, delete or update any data. If a student becomes aware that the Trust holds any inaccurate, irrelevant or out-of-date information about him/her, he/she must notify the school office and provide any necessary corrections or updates to the information.

15. **Data that is likely to cause substantial damage or distress**

i. If an employee believes that the processing of personal information about him/her is causing, or is likely to cause, substantial and unwarranted damage or distress to him/her or another person, he/she

may notify the Trust in writing to request the Trust to put a stop to the processing of that information.

ii. Within 21 days of receiving the employee's notice, the Trust will reply to the employee stating either:

- that it has complied with or intends to comply with the request; or
- the reasons why it regards the employee's notice as unjustified to any extent and the extent, if any, to which it has already complied or intends to comply with the notice.

16. **Monitoring**

i. CCTV within the schools will only be in public areas, will not intrude on anyone's privacy and be used for security purposes. Notices will be placed in the school to ensure that all visitors and staff are aware of this.

ii. The Trust may monitor employees by various means including, but not limited to, checking emails, listening to voicemails and monitoring internet use. If this is the case, the Trust will inform the employee that monitoring is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used. The employee will usually be entitled to be given any data that has been collected about him/her. The Trust will not retain such data for any longer period of time than is absolutely necessary.

iii. In exceptional circumstances, the Trust may use monitoring covertly. This may be appropriate where there is, or could potentially be, damage caused to the Trust by the activity being monitored and where the information cannot be obtained effectively by any non-intrusive means (for example, where an employee is suspected of stealing property belonging to the Trust). Covert monitoring will take place only with the approval of The Headteacher of the school or the Chair of Governors.

17. **Employees' obligations regarding personal information**

i. If an employee acquires any personal information in the course of his/her duties, he/she must ensure that:

- the information is accurate and up to date, insofar as it is practicable to do so;
- the use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
- the information is secure.

ii. In particular, an employee should ensure that he/she:

- does not share passwords or access data under someone else's credentials;
- uses password-protected and encrypted software for the transmission and receipt of emails;
- sends fax transmissions to a direct fax where possible and with a secure cover sheet; and

- lock files in a secure cabinet.

iii. Where information is disposed of, employees should ensure that it is destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in an employee's inbox or trash folder. Hard copies of information may need to be confidentially shredded and placed in the confidential waste bins. Employees should be careful to ensure that information is not disposed of in a wastepaper basket or recycle bin.

iv. If an employee acquires any personal information in error by whatever means, he/she shall inform the Headteacher immediately and, if it is not necessary for him/her to retain that information, arrange for it to be handled by the appropriate individual within the Trust.

v. Where an employee is required to disclose personal data to any other country, he/she must ensure first that there are adequate safeguards for the protection of data in the host country. For further guidance on the transfer of personal data outside the UK, please contact Mrs Marion Fletcher.

18. **Consequences of non-compliance**

i. All employees are under an obligation to ensure that they have regard to the eight data protection principles (see above) when accessing, using or disposing of personal information. Failure to observe the data protection principles within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if an employee accesses another employee's employment records without the requisite authority, the Trust may treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct may also constitute a criminal offence.

19. **Taking employment records or student attainment data off site**

i. An employee must not take any personal information away from the school's premises or their workplace (save in circumstances where he/she has obtained the prior consent of the Headteacher to do so).

ii. An employee who has been granted approval to take personal information from the school premises may take only necessary and certain records off site. These are documents relating to certain meetings that cannot be held on site, such as meetings with specific health and safeguarding professionals. An employee may also take employment records off site for any other valid reason given by the Headteacher.

iii. Any employee taking records off site must ensure that he/she complies with the Trust's 'off-site working policy' and does not leave his/her laptop, other device or any hard copies of documents on the train, in the car or any other public place. He/she must also take care when

observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information.