St Mary's Catholic High School

Records Management Policy

Created: May 2018 Review by: May 2020

Statement of Intent

St Mary's Catholic High School is committed to maintaining the confidentiality of its information and ensuring that all records within the school are only accessible by the appropriate individuals. In line with the requirements of the General Data Protection Regulation (GDPR), the school also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

The school has created this policy to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet the school's statutory requirements.

This document complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

The Data Protection Officer is Mrs L. Martin

1. Legal Framework

1. This policy has due regard to legislation including, but not limited to, the following:
   - General Data Protection Regulation (2016)
   - Freedom of Information Act 2000
   - Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)

2. This policy also has due regard to the following guidance:

1. Information Records Management Society 'Information Management Toolkit for Schools' 2016

3. This policy will be implemented in accordance with the following school policies and procedures:
2. Data Protection Policy
3. Freedom of Information Policy
4. E-security Policy
5. Security Breach Management Plan

2. Responsibilities

1. The school as a whole has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.
2. The headteacher holds overall responsibility for this policy and for ensuring it is implemented correctly.
3. The data protection officer (DPO) is responsible for the management of records at the school.
4. The DPO is responsible for promoting compliance with this policy and reviewing the policy on an annual basis, in conjunction with the headteacher.
5. The DPO is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of correctly.
6. All staff members are responsible for ensuring that any records for which they are responsible for are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

3. Management of Pupil Records

6. Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each school that a pupil attends and includes all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievement. Each child will have a paper document and an electronic file held on the MIS system (SIMs)

7. The following information is stored electronically on SIMs:
    - Forename, surname, gender and date of birth
    - Unique pupil number
    - Ethnic origin, religion and first language (if not English)

- Any preferred names
- Position in their family, e.g. eldest sibling
- Emergency contact details and the name of the pupil's doctor
- Any allergies or other medical conditions that are important to be aware of
- Names of parents, including their home address(es) and telephone number(s)
- Name of the school, admission number, the date of admission and the date of leaving, where appropriate
- Any other agency involvement, e.g. speech and language therapist
- Note of the date when the file was received
- Note of the date when the file was transferred, if appropriate

8. The following information is stored on paper in a Year Group File in the School Office:
9. Admission Form
10. Consent to attend Educational Visits for 12 months period
11. Use of Image Consent

12. The following information is stored in a pupil record in the Pastoral Office and will be easily accessible:
13. Annual written reports to parents from age 4
14. Details of SEND - SEN OFFICE
15. If the pupil has attended an early years setting, the record of transfer
16. Fair processing notice – only the most recent notice will be included
17. National curriculum and agreed syllabus record sheets
18. Notes relating to major incidents and accidents involving the pupil
19. Any information about an education and healthcare (EHC) plan and support offered in relation to the EHC plan SEN OFFICE
20. Any notes indicating child protection disclosures and reports are held
21. Any information relating to exclusions
22. Any correspondence with parents or external agencies relating to major issues, e.g. mental health
23. Notes indicating that records of complaints made by parents or the pupil are held

24. The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file for the pupil in the Pastoral Office:
25. Absence notes
26. Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.
27. Correspondence with parents about minor issues, e.g. behaviour

28. Hard copies of disclosures and reports relating to child protection are stored in a sealed envelope, in a securely locked filing cabinet in the Pastoral Office – a note indicating this is marked on the pupil's file.
29. Hard copies of complaints made by parents or pupils are stored in a file in the headteacher's office – a note indicating this is marked on the pupil's file.
30. Actual copies of accident and incident information are stored separately by the Business Manager and held in line with the retention periods outlined in this policy – a note indicating this is marked on the pupil's file. An additional copy may be placed in the pupil's file in the event of a major accident or incident.
31. The school will ensure that no pupil records are altered or amended before transferring them to the next school that the pupil will attend.
32. The only exception to the above is if any records placed on the pupil's file have a shorter retention period and may need to be removed. In such cases, the DPO is responsible for disposing of records and will remove these records.
33. Electronic records relating to a pupil's record will also be transferred to the pupils' next school. Section 10 of this policy outlines how electronic records will be transferred.
34. If any pupil attends the school until statutory school leaving age, the school will keep the pupil's records until the pupil reaches the age of 25 years.
35. The school will, wherever possible, avoid sending a pupil record by post. Where a pupil record must be sent by post, it will be sent by registered post, with an accompanying list of the files included. The school it is sent to is required to sign a copy of the list to indicate that they have received the files and return this to the school.

4. Storing and Protecting Information

1. The DPO will undertake a risk analysis to identify which records are vital to school management and these records will be stored in the most secure manner.
2. The IT Network Manager is responsible for ensuring that a daily onsite backup and off site backup occurs to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.
3. Where possible, backed-up information will be stored off the school premises, using a central back-up service.
4. Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.
5. Confidential paper records are not left unattended or in clear view when held in a location with general access.
6. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up off-site.
7. Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted.

8. All electronic devices are password-protected to protect the information on the device in case of theft.
9. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft. Staff and governors do not use their personal laptops or computers for school purposes.
10. All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
11. Emails containing sensitive or confidential information are password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email. (SSL certificate required)
12. Circular emails to parents are sent via the communication module or school app so email addresses are not disclosed to other recipients.
13. Circular emails to other professionals are sent via blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
14. When sending confidential information via email, members of staff will always check that the recipient is correct before sending.
15. Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the GDPR, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
16. Before sharing data, staff always ensure that:
    - They have consent from data subjects to share it.
    - Adequate security is in place to protect it.
    - The data recipient has been outlined in a privacy notice.

17. All staff members will implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.
18. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
19. The physical security of the school's buildings and storage systems, and access to them, is reviewed termly by the site supervisor in conjunction with the DPO. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the headteacher and extra measures to secure data storage will be put in place.
20. The school takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
21. The DPO is responsible for continuity and recovery measures are in place to ensure the security of protected data.

22. Any damage to or theft of data will be managed in accordance with the school's Security Breach Management Plan.

5. Accessing Information

St Mary's Catholic High School is transparent with data subjects, the information we hold and how it can be accessed.

All members of staff, parents of registered pupils and other users of the school, e.g. visitors and third-party clubs, are entitled to:

- Know what information the school holds and processes about them or their child and why.
- Understand how to gain access to it.
- Understand how to provide and withdraw consent to information being held.
- Understand what the school is doing to comply with its obligations under the GDPR.

All members of staff, parents of registered pupils and other users of the school and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.

Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents.

Pupils who are considered to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.

The school will adhere to the provisions outlined in the school's GDPR Data Protection Policy when responding to requests seeking access to personal information.

6. Digital Continuity Statement

1. Digital data that is retained for longer than six years will be named as part of a digital continuity statement.

2. The DPO will identify any digital data that will need to be named as part of a digital continuity statement.

3. The data will be archived to dedicated files on the school's server, which are password-protected – this will be backed-up in accordance with section 10 of this policy.

4. Memory sticks will never be used to store digital data, subject to a digital continuity statement.

5. The IT Network Manager will review new and existing storage methods annually and, where appropriate add them to the digital continuity statement.

6. The following information will be included within the digital continuity statement:

    - A statement of purpose and requirements for keeping the records
    - The names of the individuals responsible for long term data preservation
    - A description of the information assets to be covered by the digital preservation statement
    - A description of when the record needs to be captured into the approved file formats
    - A description of the appropriate supported file formats for long-term preservation
    - A description of the retention of all software specification information and licence information
    - A description of how access to the information asset register is to be managed in accordance with the GDPR

7. Information Audit

1. The school conducts information audits on an annual basis against all information held by the school to evaluate the information the school is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:
    - Paper documents and records
    - Electronic documents and records
    - Databases
    - Microfilm or microfiche
    - Sound recordings
    - Video and photographic records

- Hybrid files, containing both paper and electronic information

2. The information audit may be completed in a number of ways, including, but not limited to:
3. Interviews with staff members with key responsibilities – to identify information and information flows, etc.
4. Questionnaires to key staff members to identify information and information flows, etc.
5. A mixture of the above

6. The DPO is responsible for completing the information audit. The information audit will include the following:
    - The school's data needs
    - The information needed to meet those needs
    - The format in which data is stored
    - How long data needs to be kept for
    - Vital records status and any protective marking
    - Who is responsible for maintaining the original document

7. The DPO will consult with staff members involved in the information audit process to ensure that the information is accurate.
8. Once it has been confirmed that the information is accurate, the DPO will record all details on the school's Information Asset Register.
9. The information displayed on the Information Asset Register will be shared with the headteacher to gain their approval.

8. Disposal of Data

1. Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.
2. Where disposal of information is outlined as secure disposal, this will be shredded or pulped and electronic information will be scrubbed clean and, where possible, cut. The DPO will keep a record of all files that have been destroyed.
3. Where the disposal action is indicated as reviewed before it is disposed, the DPO will review the information against its administrative value – if the information should be kept for administrative value, the DPO will keep a record of this.
4. If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.
5. Where information has been kept for administrative purposes, the DPO will review the information again after three years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this

policy. If any information is kept, the information will be reviewed every three subsequent years.

7. Where information must be kept permanently, this information is exempt from the normal review procedures

9. Monitoring and Review

1. This policy will be reviewed on an annual basis by the DPO in conjunction with the headteacher – the next scheduled review date for this policy is December 2018.
2. Any changes made to this policy will be communicated to all members of staff and the governing board.