St Mary's Catholic High School

Data Handling Policy

Created: May 2018 Updated: May 2020 Review by: Spring 2022

Statement of Intent

St Mary's Catholic High School collects and stores personal data about staff members, pupils, parents and other individuals associated with the school. The school handles data in line with the statutory requirements outlined in the GDPR.

This procedure intends to ensure that all personal data is handled in accordance with the relevant data protection legislation.

The Data Protection Officer is Mrs L. Martin.

1. Legal framework

1.1. This policy has due regard to statutory legislation, including, but not limited to, the following:

- General Data Protection Regulation

1.2. This policy will be read in conjunction with the following school policies:

- GDPR Data Protection Policy
- Disciplinary Policy and Procedure
- E-safety Policy

- Data Security Breach Prevention and Management Plan
- GDPR Compliant Records Management Policy

2. General principles

2.1. In order to remain compliant with the GDPR, those handling data on behalf of the school are expected to:

- Consider whether they should be accessing or disclosing personal data before they do so.
- Be aware that, under the GDPR, they may be personally liable for any data disclosure.
- When transferring data to an individual or organisation, ensure they have appropriately verified that the individual or organisation are authorised to receive the data. To do this, the identity verification process will be used; however, individuals will be made aware that by doing so, they are taking personal responsibility for this process and may be required to justify their actions in the event of a complaint.
- Not discuss data held by the school with unauthorised colleagues, family members, friends or other associates of the school. Staff should check parental responsibility of SIMs before data sharing.
- Not access school records containing personal data other than for a specified purpose. Accessing personal data without a specified purpose may lead to disciplinary action or be considered as an offence under data protection legislation, leading to possible prosecution by the ICO.
- Avoid providing any specific details about individuals that might lead to their identification when using data for reports or monitoring purposes, unless they have been given written permission for this information to be used.
- Not express unsubstantiated personal opinions in file notes or emails.
- Use the blind carbon copy (BCC) option when sending out the same email to a number of people, unless recipients have agreed to share their personal email addresses with others.
- Consult their data protection officer (DPO), if necessary, before processing personal data.
- Always consider data security and the risks associated with losing personal data, before processing, downloading or printing any personal data.
- Never share or write down passwords to systems where data is stored. Doing so could result in unauthorised access to personal data and, therefore, could constitute a serious security breach.

- Ensure their passwords related to data handling systems are created in line with the school's E-safety Policy.
- Always secure devices that hold data when they are left unattended – this includes logging out of devices or services at the end of the day or when they are no longer being used. These should be Password/Pin or biometic protected.
- Take adequate precautions to protect school data in a public place – this includes protecting any mobile devices, laptops or tablets that may contain data or have the ability to access data.
- Be aware that, if adequate precautions are not taken, they are personally accepting responsibility for the associated risks and consequences if personal data is unsecure, lost, or if there is a complaint.
- Ensure no documents containing personal data are left in or on a printer, photocopier or scanner. Fax machines will not be used to transmit personal data.
- Ensure that personal data cannot be seen or accessed by unauthorised individuals.
- Ensure that paper-based data is stored in a lockable cabinet when not in use.
- Ensure that if sensitive data is being taken off the school premises, it is transported in a lockable bag or container.
- Ensure that if paper-based data is being transported by car, it is out-of-sight and stored in a secure part of the car, e.g. the boot. Paper-based data will not be left in a car overnight. If data is stored at home, it will be kept in a locked or secure container.
- Dispose of paper-based personal data either in appropriate waste bins that are not accessible by unauthorised individuals or by shredding the documents. If large amounts of paper-based data not stored on the school premises requires disposal, the Business Manager/DPO will be consulted to ascertain a secure disposal option.
- Ensure that personal data is encrypted.
- Only extract personal data with prior approval from the Business Manager/DPO.
- Seek written authorisation from the Headteacher or the DPO prior to extracting more than 1,000 personal data records or 10 sensitive personal data records.
- Laptops taken off site must have encrypted hard drives
- All staff should lock their PC when leaving a room (It is possible to set a system wide default auto lock).
- Users should not be logged on as someone else (ie each person should have their own username and password to access systems to ensure

each individual has the correct rights and does not have access to information they are not authorised to view).

- Print sensitive documents from photocopiers that pupils don't have access to in case of paper jams, printer problems to avoid unattended print of all documents in queue when the problem has been fixed.
- Teachers should freeze the projector image or use extended desktop (if available) to prevent class pupils from seeing sensitive information regarding children on their computer desktop.
- Turn off email preview on class computes to prevent potentially sensitive information being displayed on a projector screen.
- Take immediate action in the event of a data breach and report any breaches to the DPO.

3. Transfer of data to a third-party data processor

3.1. A formal written data processing agreement will be in place before personal data is transferred to a third-party data processor. The agreement will state:

- The data processor's obligation to treat the data in line with data protection legislation.
- The reasons for the transfer.
- The time period for the transfer.
- The purpose for which the data is required.
- How the data will be processed.
- What actions will be taken to dispose of the data when it is no longer needed.

3.2. The DPO is responsible for initiating and managing data processing agreements, and other members of staff will check with the DPO that there is an agreement in place before organising a transfer.

3.3. Data processing agreements are only valid within the European Economic Area; any other transfers are not permissible unless other arrangements are made.

3.4. Once an agreement is in place, data that is to be transferred will be made secure. The school takes reasonable precautions to protect data during transfer, such as encryption.

3.5. If data is being transferred via the postal service, it will only be sent using a secure courier or special delivery service. The recipient of the data will be clearly stated and the party requesting the data will be required to fund postage costs.

3.6. If data is sent via a courier or special delivery service, the intended recipient will be advised of when to expect the data and they will confirm safe receipt as soon as the data arrives. The sender is responsible for ensuring that the confirmation is received and for liaising with the courier service if there is any delay in the receipt of the data.

3.7. When transferring data directly from one server to a remote serve don't use the admin 'default' account, create a new username and a password that only has sufficient rights and privileges necessary to transfer the data.
3.8. Periodically review data that is being sent to ensure it is still valid.

4. Storing personal or sensitive personal data externally

4.1. Through its Management Information (SIMs) system, the school processes its personal data daily to assist and support staff members.
4.2. The GDPR requires that all departments have appropriate security in place to protect personal data against unlawful or unauthorised use or disclosure, accidental loss, destruction or damage.
4.3. The DPO is responsible for identifying and implementing appropriate security measures to protect the personal data stored on the MI system or other data repositories.
4.4. Any instances of stored or transferred data that are found to be unsecure will be immediately reported to the DPO who will secure that data immediately.
4.5. The use of pen drives and external hard drives is strictly prohibited.
4.6. Don't use any personal cloud storage such as dropbox as other family members may have rights to view your storage and consequently these documents. All staff have secure cloud storage as part of their Office 365 account.

5. Confidentiality

5.1. Any member of staff or other person associated with the school that handles or shares data will adhere to the following principles:

- The purpose for sharing data is justified
- Data that personally identifies individuals is not used unless absolutely necessary
- Data is only disclosed on a need-to-know basis – Check account details of contact list.
- Guidance is sought from the DPO as appropriate

5.2. If personal data is being communicated verbally in person, it will not be shared in front of other individuals who are not authorised to access the data.
5.3. Staff members will not disclose or request the disclosure of sensitive data about themselves or others in areas where there are likely to be unauthorised people present, e.g. the school reception, or discussing with other staff members at break in the corridor.

5.4. Disclosure of data via the telephone will be conducted in line with the following procedures:

- Verify the identity of the other party on the phone – the type of verification will differ by service and the sensitivity of the data being disclosed
- Establish the reason for requesting the data and ensure this is appropriate
- Where appropriate, request the other party's contact details and check their identity by calling the person via their organisation's main switchboard and asking for them by name
- Only provide the data to the person who requested it
- Do not disclose any personal data via voicemail – be aware that confirming you are a member of the school could be considered as releasing personal information
- Take precautions to ensure that data is not shared inappropriately with others, e.g. be cautious if disclosing data on the phone when in a public place
- Do not disclose sensitive personal data via text messaging
- Do not disclose the reason staff are absent from school
- Ensure the door is closed before starting a confidential conversation concerning personal data

5.5. Disclosure of data via email will be conducted in line with the following procedures:

- Sensitive personal data (or bulk records) will be encrypted if sent via email
- Emails containing non-sensitive personal data about less than 10 data subjects do not need to be encrypted unless the data subject requests that communication is encrypted
- Test emails will be sent before sending sensitive (or bulk) data
- Bulk data will not be separated into smaller sets to avoid the requirement for encryption
- Care will be taken when addressing emails to ensure a correct, current address is used and the email is only sent to those with a legitimate interest
- If data is not received by the intended recipient, the contact details and email addresses will be checked to ensure they are correct before resending

- Consider what impact any data being lost or misdirected may have – where data is being provided in bulk or is of a sensitive nature, an assessment will be made on the type of protection to be applied
- Avoid putting sensitive personal information about more than one person in an email as this will lead to difficulties in maintaining accurate and relevant individual employee's records
- When transferring data, be aware of who has permission to view your emails or who might be able to view your recipient's emails
- Emails containing sensitive data relating to a single individual do not need to be encrypted

5.6. Paper-based data will be managed as follows:

- The school implements a clear-desk policy wherever possible and staff members will ensure that their desks are clear of documents containing personal data at the end of each day
- All files containing personal data will be stored in locked filing cabinets, cupboards or drawers
- Sensitive data will be held securely at all times, i.e. stored in a locked filing cabinet, cupboard or drawer and in a locked bag if the data is being transported,
- A tracer card system will be used when removing a file from its storage – the card will be inserted in place of the file identifying the file removed, the holder of the file and the expected return date.

6. Managing Systems

6.1. All department work to be stored on the W Drive>Department Name
6.2. Curriculum Leader to be responsible for folder storage
6.3. Business Support to store work in O Drive>Office or J Drive>Finance dependent upon responsibilities
6.4. X Drive Staff should be used only for items not related to departmental work
6.5. All documents **must** contain path file information.
6.6. All documents containing personal data must have a retention period or destruction date clearly displayed in the footer

7. Use of Email (Refer to Email Policy)

7.1. Blanket emails are not permitted. Must be sent on a need to know basis.
7.2. When sending internal email messages that contain personal data. The document should be stored on W Drive and hyperlink attached to email, if email sent in error, anyone outside of the organisation cannot access the information.

7.3. Emails containing personal data to external users should be sent via secure email or be encrypted.
7.4. Consider delayed send, test send or send for review when using bulk email.
7.5. Don't use your email account as a filling system.
7.6. Delete emails that are no longer required.
7.7. Staff should only send personal data from school email addresses

8. Monitoring and review

8.1. This policy will be reviewed by the headteacher and DPO on an annual basis.
8.2. The next scheduled review date for this procedure is April 2019.