The St Michael Steiner School

Data Protection Policy

Introduction

Staff, pupils, parents and visitors provide personal information in order that the school can fulfil its stated purpose and responsibilities in educating children both now and into the future. It is the school's duty to ensure that this personal data is held securely and used responsibly.

The intention of this policy is not to restrict the legitimate use of personal data, but to raise awareness of what information we collect about people and why we need it, so that we do not ask for or store information that we don't need, or share it with people who don't need to see it.

The aim of this policy and its procedures is rather to enable staff to continue to fulfil to the best of their ability their commitment to the children in their care, toward the school, their colleagues, the children's parents and visitors to the school, while at the same time complying with the General Data Protection Regulation (GDPR) (May 2018)[1], which regulates the way the school:

- collects personal information
- stores the information
- shares the information with third parties
- justifies its collection, sharing and storage
- disposes of information that is no longer needed
- informs people of what information is being collected, why, for how long it will be kept, with whom it will be shared and how they can access their own and their children's data.

Data Processing

The activities above are referred to in GDPR legislation as 'processing'; when we handle personal data, we become 'data processors'. In our school, all staff are data processors, therefore, all staff must understand how to handle data in accordance with school policy and develop good practice out of this understanding.
The school is responsible for ensuring that data is handled according to its policy and procedures. Decisions about how staff process data are made by the College, acting as the Data Controller, and ratified by the Trustees. The Data Controller is responsible for the following and appoints a Data Protection Officer (DPO) to act on its behalf in:

- monitoring how data is being handled in the school
- devising their own procedure for doing this
- advising staff in a 'troubleshooting' capacity
- enabling people to have access to their own personal data (Subject Access Requests or SAR)
- reporting and handling security breaches
- ensuring that staff are trained in data processing and that regular training is made available to everyone

[1] In addition to data protection legislation, the school has to comply with other legislation including the Education Act (2002, 2011), The Children Act (2004), The Childcare Act (2006), the Safeguarding Vulnerable Groups Act (2006) and The Prevent Duty (2015), all of which supersede the GDPR.

- creating and updating this policy and procedure for handling personal data and notifying staff of any changes
- ensuring that the procedures in this policy are followed
- updating the Policy for the Processing and Retention of Personal Data as needed and notifying staff of any changes
- keeping a record of the hardware on which each staff member is storing personal data
- ensuring permanent destruction of hard copies of material containing personal data
- taking possession of external hard drives, memory sticks and email accounts of staff when they leave the school permanently and ensuring they are wiped securely by an approved company

The Data Protection Officer (DPO) is registered with the Information Commissioner's Office (ICO)

See the document 'Guidance for the Data Protection Officer' for more detailed information about the role.

The school's designated Data Protection Officer is Stuart Purdy

Data Protection Impact Assessment

As the Data Controller, the school must have a lawful basis on which to collect, store, share and dispose of any personal data. See the school's Policy for the Processing and Retention of Personal Data for details of the different kinds of data the school collects, on what lawful basis and for how long it is held.

If staff encounter a processing activity involving personal data which does not fall under one of the categories listed in the policy, or if a processing activity changes, s/he should consult the DPO.

If the activity is considered likely to result in "a high risk to the rights and freedoms" of the people concerned, a Data Protection Impact Assessment (DPIA) must be carried out, using the DPIA form.

For information about activities likely to need a DPIA see: https://ico.org.uk/for- organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact- assessments-dpias/when-do-we- need-to-do-a-dpia/

The completed DPIA form should be passed to the DPO who will bring it to the College for ratification and add it to the Policy for the Processing and Retention of Personal Data.

If the risks cannot be successfully mitigated, the processing activity may not be allowed, or the DPO will submit the DPIA to the Information Commissioner for assessment.

For examples of processing activities that may be high risk see: https://ico.org.uk/for-organisations/guide- to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of- processing-likely-to-result-in-high-risk/

Procedure for staff

For comprehensive advice on all aspects of GDPR, see the GDPR Toolkit for Schools in the policies folder.

All staff must take the online training 'A Practical Guide to the GDPR for Education'[2] and obtain a certificate showing that they are able to process data properly.

[2] Or similar training offered by another provider.

This training is provided by the school through its subscription to *Educare*; all staff are given a password to access it. Please contact the DPO if you do not have one.

This training should be updated annually and certificates placed in the relevant staff files.

When handling personal data, staff should refer to the procedures below and to the Policy for the Processing and Retention of Personal Data for guidance.

Personal data about staff, pupils, parents and visitors must not be disclosed to any third party, either deliberately or accidentally, except under the conditions laid out in the Policy for the Processing and Retention of Personal Data.

Storing, using and disposing of personal data securely

All personal data provided to the school about staff, pupils, parents, visitors or anyone else, must be held and used securely in order to prevent accidental disclosure to third parties.

Electronic data

School-related personal data must be stored securely on password-protected hardware.

Electronically-held personal data must only be used on password-protected/encrypted hardware.

Information about how long different items of data may be kept is in the Policy for the Processing and Retention of Personal Data

When electronically-held personal data reaches the end of its retention period, the user (data processor) must delete it from their password protected/encrypted computer, external hard drive or memory stick. In practice, this will only need to be done at the end of a school year in most cases.

If no other copy of the deleted data exists, the Record of Data Destroyed must be completed and passed to the DPO.

Hard copies of data

Hard copies (paper) of documents containing personal data must be stored in files or folders in a locked filing cabinet in the school office or Finance office.

When hard copies of data are no longer needed the user should post them into the personal data disposal box in the school office for disposal by the DPO

Hard copies of information handed out at meetings, e.g. meeting agendas, finance information, must be returned to the person who issued them at the end of the meeting. They are then responsible for disposing of them as above.

Hard copies of personal data must be disposed of by the DPO who will follow the procedure in the Policy for the Disposal of Personal Data.

Only school staff are authorised to go into the school offices; no unauthorised personnel are allowed into the offices unaccompanied.

School offices must be kept locked at all times when unoccupied.

Taking personal data off site

We acknowledge that staff need to do a considerable amount of work at home in order to fulfil their duties, and that this will sometimes involve taking hard copies of personal data off site. There is no legislation prohibiting this, but it is the duty of the school to ensure that personal data is secure and legitimately used under all circumstances.

Generally, it is much easier and safer to take data off site electronically than to take hard copies.

You may take personal data home under the following conditions:

- The personal data taken off site is necessary in order for you to carry out your work
- Your personal computer or tablet is password protected at all times while using personal data
- The personal data is not transferred to any hardware that is not password-protected/encrypted at any time
- You do not use public wifi or internet providers to access or send personal data (e.g. in a café or library) as these are not secure.
- You do not disclose, either deliberately or accidentally, the personal data to any third party except under the conditions laid out in the Policy for the Processing and Retention of Personal Data.
- When you take pupils' written work off site, e.g. for marking, you should be aware of any possible breach of security and handle the documents appropriately.[3]
- Since information on paper cannot be secured in the way electronic data can, you do not take personal data (other than pupils' work) in the form of paper documents off site unless it is absolutely necessary. If you must in order to fulfil your duties, you keep these in your possession at all times and return them to school to be stored properly when you have finished with them.
- You fill in the Personal Data Removal form on the filing cabinets in the offices when removing hard copies of personal data (except pupils' work). (see below re making copies)
- Hard copies of Special Category Data are not taken off site under any circumstances. If this seems unavoidable, the documents can be scanned and taken electronically and deleted when they are no longer needed.
- If there is a breach of security involving data you have taken off site, you inform the DPO and co-operate in the Personal Data Breach Handling Procedure

Copying personal data

It is sometimes necessary to make copies or scans of documents containing personal data, for example, when application forms arrive, they are copied and given to the relevant teachers. Copies must be handled in the same way as the originals.

When you make a copy or scan of any document containing personal data you must:

- Record its creation on the Personal Data Removal/Duplication form next to the photocopier
- When the copies are no longer needed, post them into the personal data disposal box in the school office for disposal by the DPO
- Record that you have done this on the Personal Data Removal/Duplication form

Emailing personal data

All staff should have a school email address which must be used for all school correspondence; if you do not have one, contact the DPO. Do not email any personal data until you have it.

Email addresses of staff, parents, pupils and visitors must be held in the address book in your school email account, not your personal one.

If emailing personal data to colleagues, you must use your, and their, school email address.

---

[3] Pupils' work does not usually contain personal data, but sometimes it may, e.g. pupils may write about their parents' work; older pupils may express political (etc.) opinions.

If emailing personal data to third parties (under the conditions laid out in the Policy for the Processing and Retention of Personal Data) you must do so using your school email address.

Personal email addresses must not be used to send personal data under any circumstances; if this happens accidentally, or if you receive someone else's personal data via your personal email address, you must delete the email and reply requesting that the sender uses your school email address.

Sending personal data to GDPR regulated countries

Personal data is sometimes sent to countries where the GDPR does not apply, e.g. when pupils move to those countries and the destination school asks for references and records to be sent. In this case, the Data Controller must assess whether it is safe to send the information. (See guidance: https://ico.org.uk/for-organisations/guide-to- data-protection/principle-8-international/#not-approved)

In most cases, the safest way to transfer the information is to send it to the pupil's parents who can then pass it on to the new school.

In the case of Child Protection records (parents are often legitimately not given access to safeguarding information) advice must be sought from the school's Safeguarding Lead before sending anything.

CSE Assessment information for High School students is uploaded to the SEDT Google Drive for moderation and certification in New Zealand. The school is satisfied that the system used to store and process their data is secure. [see the SEDT/SMSS contract document section 10.1, available from the CSE co-ordinator]

When staff leave the school

If you leave the school, you no longer have a legitimate reason to hold personal data relating to people in the school community. The DPO will:

- Take possession of or delete your school email address and its contents (sent and received emails, address book)
- Ensure that school-related personal data is removed from your computer, memory stick and/or external hard drive and store the information as is appropriate in each case.
- Ask you to return hard copies of any school-related personal data in your possession, as you are contractually obliged to do.

Data formerly held on personal computers

Data stored on personal computers will still be retrievable from your hard drive even after you have deleted it. Any computer that has ever held school-related personal data should be returned to the school at the end of its useful life for secure wiping and/or disposal. This is a contractual obligation.

Internal security

Some data needs to be available to all staff in order that they can do their work; some does not.

Staff should be aware of who needs to have access to the data they hold and process and not disclose it to anyone who does not need to see it. e.g. by leaving documents open on open laptops or sending emails to all staff unnecessarily.

Electronically stored, password-protected, encrypted data will be safe from accidental disclosure in the school as well as externally.

Hard copies of data to which access needs to be restricted, e.g. Child Protection files, should be kept in separate, locked files in the school office or the Finance office. (See Safeguarding and Child Protection policies)

If it is necessary to print or photocopy personal data, you must be present in the office yourself to collect it when it comes out of the machine, and, if there is a 'log jam' of work and you can't wait, to delete it until you can be there.

If there is a breach of security, you must inform the DPO and co-operate in the Personal Data Breach Handling Procedure

If there is a security breach

If you are aware of any breach of security involving personal data, you must inform the DPO immediately and co-operate in the Personal Data Breach Handling Procedure.

Subject Access Requests (SAR)

Anyone may ask for access to their own or their child(ren)'s personal data at any time. The DPO must respond to this request in writing (in print or by email) within 40 days, but preferably sooner.

Staff must co-operate with the DPO in responding to an SAR. In order to do this, all personal data relating to students, staff, parents and visitors must be stored in an organised way so that it can be accessed promptly.

Other regulations, policies and procedures referred to in this document:

These documents are available from the DPO: .

General Data Protection Regulation (GDPR) (May 2018)

Policy for the Processing and Retention of Personal Data

Personal Data Breach Handling Procedure

Personal Data Removal/Duplication form

Record of Data Destroyed

Guidance for the Data Protection Officer

Privacy/Data Protection statements from agencies to which the school provides personal data

DPIA form

GDPR Toolkit for Schools

Useful links
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection- regulation-gdpr/
https://ico.org.uk/for-organisations/data-protection-act-2018/

This policy is drawn up with reference to: https://ico.org.uk/media/for-organisations/ documents/ 2014223/
subject-access-code-of-practice.pdf Review date: February 2021