



St. Michael's School

**Data Protection / Record Retention
Policy**

January 2021

St. Michael's School

Data Protection / Record Retention Policy

Introductory Statement

The purpose of St. Michael's School's Data Protection Policy is to support the school in meeting its responsibilities with regard to the processing of personal data held by the school's Board of Management (BoM). These responsibilities arise as statutory obligations under the relevant data protection legislation, the Data Protection Acts 1988 to 2018 and the EU General Data Protection Regulation (GDPR). They also stem from our desire to process all personal data in an ethical manner which respects and protects the fundamental rights and freedoms of natural persons.

This Data Protection Policy is updated to include General Data Protection Regulation – GDPR and Child Safeguarding in the Online Space, as the school community engage with remote learning during school closures related to COVID-19.

The school recognises the seriousness of its data processing obligations and has implemented a set of practices to safeguard personal data. Relevant policies and procedures apply to all school staff, boards of management, trustees, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the school) insofar as the measures under the policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and special categories of personal data will be protected by the school.

St. Michael's School operates a “*Privacy by Design*” method in relation to Data Protection. This means we plan carefully when gathering personal data so that we build in the *data protection principles* as integral elements of all data operations in advance. We audit the personal data we hold in order to:

1. be able to provide access to individuals to their data
2. ensure it is held securely
3. document our data protection procedures
4. enhance accountability and transparency.

Data Protection Principles

The school Board of Management is a *data controller* of *personal data* relating to its past, present and future staff, students, parents/guardians and other members of the school community. As such, the BoM is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 to 2018 and GDPR, which can be summarised as follows:

- **Data will be processed lawfully, fairly and in a transparent manner;**

Obtain and process Personal Data lawfully, fairly and in a transparent manner, Information on students is gathered with the help of parents/guardians and staff. Information is also transferred on occasion from their previous schools. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the School, parents/guardians of students, etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the School. All such data is treated in accordance with the Data Protection legislation and the terms of this Data Protection Policy.

- **Data will be collected for specified, explicit and legitimate purposes;**

Keep it only for one or more specified and explicit lawful purposes- The BoM will inform individuals of the reasons they collect their data and the uses to which their data will be put. All information is kept with the best interest of the individual in mind at all times.

- **Data will be processed only in ways compatible with the purposes for which it was given initially;**

All data is processed in a manner consistent with the purposes for which it was gathered. Information will only be disclosed on a 'need to know' basis, and access to it will be strictly controlled.

- **Data will be adequate, relevant and limited to what is necessary;**

Ensure that it is adequate, relevant and not excessive- Only the necessary amount of information required to provide an adequate service will be gathered and stored.

- **Data will be accurate and, where necessary, kept up to date;**

Keep Personal Data accurate, complete and up-to-date- Students, parents/guardians, and/or staff should inform the school of any change which the school should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, complete and up-to-date. Once informed, the school will make all necessary changes to the relevant records. Records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration(s) to be made to any original record/documentation should be dated and signed by the person making that change.

- **Data will be kept for no longer than is necessary;**

Retain it no longer than is necessary for the specified purpose or purposes for which it was given- As a general rule, the information will be kept for the duration of the individual's time in the school. Thereafter, the school will comply with the Department of Education and Skills' (DES) guidelines on the storage of Personal Data and Sensitive Personal Data relating to a pupil. In the case of members of staff, the school will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The school may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and or/defending a claim under employment legislation and/or contract and/or civil law. See Appendix 1, School Record Retention Schedule for St. Michael's School.

- **Data will be processed in a manner that ensures appropriate security;**

Keep Personal Data safe and secure-

Only those with a genuine reason for doing so may gain access to the information. Personal Data is securely stored under lock and key in the case of manual records and protected with computer software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) are encrypted and password-protected.

- **Consent will be provided;**

Where consent is the basis for provision of personal data, (e.g. data required to attend/participate in school trips or events) the consent must be a freely-given, specific,

informed and unambiguous indication of the data subject's wishes. St. Michael's School will require a clear, affirmative action e.g. ticking of a box/signing a document to indicate consent. Consent can be withdrawn by data subjects in these situations.

- **A copy of all data will be provided to the individual on request;**

Individuals have a right to know and have access to a copy of personal data held about them, by whom, and the purpose for which it is held.

Scope

The Data Protection legislation applies to the keeping and processing of *Personal Data*. The purpose of this policy is to assist the school to meet its statutory obligations, to explain those obligations to School staff, and to inform staff, students and their parents/guardians how their data will be treated.

The policy applies to all school staff, the Board of Management, parents/guardians, students and others (including prospective or potential students and their parents/guardians, and applicants for staff positions within the school) insofar as the school handles or processes their *Personal Data* in the course of their dealings with the school.

Definition of Data Protection Terms

In order to properly understand the school's obligations, there are some key terms, which should be understood by all relevant school staff:

Personal Data means any data relating to an identified or identifiable natural person i.e. a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller (BoM).

Data Controller is the Board of Management of the school

Data Subject - is an individual who is the subject of personal data

Data Processing - performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data,
- Collecting, organising, storing, altering or adapting the data
- Retrieving, consulting or using the data
- Disclosing the data by transmitting, disseminating or otherwise making it available
- Aligning, combining, blocking, erasing or destroying the data

Data Processor - a person who processes personal information on behalf of a data controller, but **does not include an employee of a data controller** who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection legislation places responsibilities on such entities in relation to their processing of the data, e.g. Aladdin, Paschal Software, the school accounting/wages processors, etc.

Special categories of Personal Data refers to *Personal Data* regarding a person's

- racial or ethnic origin
- political opinions or religious or philosophical beliefs

- physical or mental health
- sexual life and sexual orientation
- genetic and biometric data
- criminal convictions or the alleged commission of an offence
- trade union membership

Personal Data Breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. This means any compromise or loss of personal data, no matter how or where it occurs.

Implication of the Current Situation in relation to how schools operate remotely during school closures in relation to Covid-19

Staff must operate within the remits of the school's policies and practices. Our policies are being reviewed and updated taking cognisance of online/distance activities as detailed in our 'Action Plan for Remote Learning'.

As detailed in our updated Acceptable Use Policy (AUP) for pupils, online network platforms permissible for use by staff include Zoom, Seesaw and G-Suite (Google Classroom). Parental/pupil consent is necessary.

As part of its delivery of remote learning, staff are organising a series of virtual classroom events to allow teachers, SNAs and students to interact in real time using the Zoom videoconferencing platform. Teachers will communicate the details and scheduled times to students and parents by email using their work email address. Care is needed to ensure the online security of everyone involved. Students are reminded that all of the school's policies, notably the Code of Behaviour and the Acceptable Use Policy, apply during these online lessons. As the virtual classroom provides an opportunity for participation, teachers encourage some audio and/or video interaction with students. Students are being advised of best practice around this participation e.g. quiet location, proper attire, no personal information visible in background (bedrooms etc. best avoided) etc.

No live recordings will be done using Zoom videoconferencing platform. This is to respect the personal data of all, both teachers and students, who participate in each virtual lesson. All are reminded that no recording (or screen photograph) of any part of the video lesson should be made by any other means. The recording and onwards sharing of personal data would be unlawful as well as a contravention of the school's policies.

The school appreciates home support to ensure that best learning outcomes are achieved while also respecting everybody's privacy at home. Any work sent via email on Seesaw/Google Classroom will be deleted at the end of the school closure period/or as deemed appropriate in line with the pupils' e-portfolio, e.g. at the end of the Junior Cycle Level 2 Programme. Any other work that needs to be maintained will be printed. Videos of students reading or completing exercises or activities will be deleted at the end of the school closure.

Communication between staff and parents will be via emails and between staff members will be via email or Aladdin, the school approved communication service. Communication from the school to parents will be via SMS or email via the Aladdin system. Staff will adhere at all times with Child safeguarding procedures, i.e. no unapproved personal contact with students and all communications should use “work” email addresses rather than personal emails. Emails will be deleted at the end of each school year. Class teachers will contact families by telephone once a week, blocking their own phone ID number.

Teachers should only use the schools trusted networks or cloud services and comply with any rules and procedures about cloud and network access, login details and data sharing. Our school is signed up to G –suite, Zoom and Seesaw and as part of the sign-up process, the school was offered and accepted a Data Processing Agreement that will address many of the major compliance issues (GDPR Article 28). Ad-hoc use of apps or services by individual teachers is discouraged. The digital age of consent is 16.

Teachers are permitted to bring class laptops home in consultation with the Principal, for use as appropriate, during periods of school closure and remote learning with students. Staff using their own devices at home, cannot store student data on them, including images of children engaged in learning activities. Great care is needed when any personal data is stored on a school device. Staff must ensure device screens are not visible to others when personal data is being accessed and screen savers should automatically activate when the device is not in use. Care is exercised around the security and use of any mobile devices.

Staff are reminded of Child Safeguarding procedures, AUP, Code of Behaviour and its addendum, Action Plan for Remote learning. In line with the review of our school’s Child Safeguarding Statement at this time, staff are advised when handling a concern or disclosure, to follow the Child Safeguarding Procedures. Where it is not possible to jointly report a concern with the Designated Liaison Person (DLP), the teacher/SNA should make their own report directly to Tusla and provide a copy of that report to the school DLP. For further information, visit www.tusla.ie/children-first/contact-a-social-worker.

Rationale

In addition to its legal obligations under the broad remit of educational legislation, the school has a legal responsibility to comply with the Data Protection Acts 1988 to 2018 and the GDPR.

This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with whom it will be shared. The school takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual’s personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the Principal and Board of Management to make decisions in respect of the efficient running of the School. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the school and Board of Management.

Other Legal Obligations

Implementation of this policy takes into account the school's other legal obligations and responsibilities. Some of these are directly relevant to data protection. **For example:**

Under **Section 9(g) of the Education Act, 1998**, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education.

Under **Section 20 of the Education (Welfare) Act, 2000**, the school must maintain a register of all students attending the School.

Under **Section 20(5) of the Education (Welfare) Act, 2000**, a Principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the Principal of another school to which a student is transferring. [Ainm na Scoile] sends, by post, a copy of a child's *Passport*, as provided by the National Council for Curriculum and Assessment, to the Principal of the Post-Primary School in which the pupil has been enrolled.

Where reports on pupils which have been completed by professionals, apart from [Ainm na Scoile] staff, are included in current pupil files, such reports are only passed to the Post-Primary school following express written permission having been sought and received from the parents of the said pupils.

Under **Section 21 of the Education (Welfare) Act, 2000**, the school must record the attendance or non-attendance of students registered at the school on each school day.

Under **Section 28 of the Education (Welfare) Act, 2000**, the School may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, Tusla, the National Council for Special Education and other schools). The BoM must be satisfied that it will be used for a 'relevant purpose' (which includes recording a person's educational or training history or monitoring their educational or training progress; or for carrying out research into examinations, participation in education and the general effectiveness of education or training).

Under **Section 14 of the Education for Persons with Special Educational Needs Act, 2004**, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers) such information as the Council may from time to time reasonably request.

The **Freedom of Information Act 2014** provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data", as with data protection legislation. While most schools are not currently subject to freedom of information legislation, (with the exception of schools under the direction of Education and Training Boards), if a school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed by that body if a request is made to that body.

Under **Section 26(4) of the Health Act, 1947** a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection.

Under ***Children First Act 2015***, mandated persons in schools have responsibilities to report child welfare concerns to TUSLA- Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

Relationship to Characteristic Spirit of the School

St. Michael's School seeks to:

- enable students to develop their full potential
- provide a safe and secure environment for learning
- promote respect for the diversity of values, beliefs, traditions, languages and ways of life in society

We aim to achieve these goals while respecting the privacy and data protection rights of students, staff, parents/guardians and others who interact with us. The school wishes to achieve these aims/missions while fully respecting individuals' rights to privacy and rights under the Data Protection legislation.

Personal Data

Records are held both on paper and electronically. The school uses the 'Aladdin' system, which is fully compliant with GDPR. The same considerations of data protection apply regardless of format of personal data (whether paper or digital). The Board of Management as data controller determines the level of access available to these records.

The *Personal Data* records held by the school **may** include paper records, electronic record and/or records stored on Aladdin. The same considerations of data protection applies regardless of format of personal data (whether paper or digital):

A. Staff records:

Categories of staff data:

As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. These staff records may include:

- Name, address and contact details, PPS number.
- Name and contact details of next-of-kin in case of emergency.
- Original records of application and appointment to promotion posts
- Details of approved absences (career breaks, parental leave, study leave, etc.)
- Details of work record (qualifications, classes taught, subjects, etc.)
- Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties
- Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under Children First Act 2015
- Details required in relation to employment matters as required in compliance with labour legislation

Purposes:

Staff records are kept for the purposes of:

- the management and administration of school business (now and in the future)

- to facilitate the payment of staff, and calculate other benefits/entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant)
- to facilitate pension payments in the future
- human resources management
- recording promotions made (documentation relating to promotions applied for) and changes in responsibilities, etc.
- to enable the school to comply with its obligations as an employer, including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the Safety, Health and Welfare at Work Act 2005)
- to enable the school to comply with requirements set down by the Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies
- and for compliance with legislation relevant to the school.

Location and Security procedures of St. Michael's School:

Manual records are kept in a secure, locked filing cabinet in a locked administration office only accessible to personnel who are authorised to use the data. Employees are required to maintain the confidentiality of any data to which they have access.

Digital records are stored on password-protected computers with adequate encryption and firewall software in a locked office. The school has the burglar alarm activated during out-of-school hours.

B. Student records:

Categories of student data:

These may include:

- Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the school. These records may include:
 - name, address and contact details, PPS number
 - date and place of birth
 - names and addresses of parents/guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
 - religious belief
 - racial or ethnic origin
 - membership of the Traveller community, where relevant
 - whether they (or their parents) are medical card holders
 - whether English is the student's first language and/or whether the student requires English language support
 - any relevant special conditions (e.g. special educational needs, dietary needs, health issues and where applicable, medical indemnity forms, etc.) which may apply

- Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student)
- Psychological, psychiatric and/or medical assessments
- Multidisciplinary reports (speech and language, occupational therapy, physiotherapy, and/ or social work services);
- Information on intervention programmes/ supports provided by external agencies for example, Irish Society for the Prevention of Cruelty to Children (ISPCC), National Educational Psychological Service (NEPs), Child and Adolescent Mental Health Service (CAMHS), Children at risk in Ireland (CARI) etc.
- Individual Education Plans
- Attendance records
- Photographs and recorded images of students (including at school events and noting achievements) are managed in line with the accompanying policy on school photography.
- Academic record – subjects studied, class assignments, examination results as recorded on official School reports
- Records of significant achievements
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Other records e.g. schools outing records, intimate care reports, records of any serious injuries/accidents, etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
- Records of any reports the school (or its employees) have made in respect of the student to State Departments and/or other agencies under Children First Act 2015.

Purposes:

The purposes for keeping student records include:

- to enable each student to develop to his/her full potential
- to comply with legislative or administrative requirements
- to ensure that eligible students can benefit from the relevant additional teaching or financial supports
- to support the provision of religious instruction
- to enable parents/guardians to be contacted in the case of emergency or in the case of school closure, or to inform parents of their child's educational progress or to inform parents of school events, etc.
- to meet the educational, social, physical and emotional requirements of the student
- photographs and recorded images of students are taken to celebrate school achievements, e.g. compile yearbooks, establish a school website, record school events, and to keep a record of the history of the school. Such records are taken and used in accordance with the 'School Photography Policy' and 'School Website Privacy Statement'.
- to ensure that the student meets the school's admission criteria
- to ensure that students meet the minimum age requirement for attendance at Primary School.
- to ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities

- to furnish documentation/information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and other schools, etc. in compliance with law and directions issued by government departments
- to furnish, when requested by the student (or their parents/guardians in the case of a student under 18 years) documentation/information/references to second-level educational institutions.

Location and Security procedures:

Manual records are kept in a secure, locked filing cabinet in a locked administration office only accessible to personnel who are authorised to use the data. Employees are required to maintain the confidentiality of any data to which they have access. Access to the information is strictly controlled and made available only to those rightfully entitled to it as detailed above. A record folder is maintained in the office to record and track all pupils' files taken. Teachers are required to sign for any files removed from the School Office. Pupils' files are not permitted to be removed from the school building and must be returned to the office on the same day they are removed. Teachers removing these files must ensure that the confidentiality of these records is always maintained.

Each teacher is provided with a pupils' folder containing active documents (e.g. current Individual Education Plans, care plans, medical needs/protocols etc). This folder is accessible to Special Needs Assistants and other teachers working directly with the pupils and is kept in a locked press in the classroom.

Digital records are stored on password-protected computer with adequate encryption and firewall software in a locked office. No personal data/ files should be stored on class laptops or on computers in the computer room or around the school. All devices used to access student data or school administrative communication should be encrypted and protected against virus'. Passwords for accessing Aalddin or other online platforms must not be disclosed to anyone. Staff are advised against the use of USB sticks. Hard drives are available for storing a backup of electronic records and are securely stored in a locked press in the office. The school is exploring the use of the icloud for storage as advised. The school has the burglar alarm activated during out-of-school hours.

C. Board of Management records:

Categories of Board of Management data:

- Name, address and contact details of each member of the Board of Management (including former members of the Board of Management)
- Records in relation to appointments to the Board
- Minutes of Board of Management meetings and correspondence to the Board which may include references to individuals.

Purposes:

To enable the Board of Management to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of Board appointments and decisions.

Location and Security procedures of St. Michael's School:

Manual records are kept in a secure, locked filing cabinet in a locked administration office only accessible to personnel who are authorised to use the data. Employees are required to maintain the confidentiality of any data to which they have access.

Digital records are stored on password-protected computer with adequate encryption and firewall software in a locked office. The school has the burglar alarm activated during out-of-school hours.

D. Other Records:

Administrative Data:

- Attendance Reports, Roll Book, Registers.
- Accident/Illness Report Book.
- Administration of Medicines Indemnity Form.
- Minutes of all staff meetings.
- Minutes of all Board of Management meetings.
- Whole School Plan
- Files Record Book
- School Outings Record
- Minibus Record of Mileage and use
- Medication Record
- Visitors Record

Telephone numbers and addresses are not released without prior consent of the parties involved.

Financial records- Current financial records are retained in the School Office with relevant older records retained in accordance with legislation.

Purposes:

The purposes for keeping administrative records are:

This information is required for routine management and administration of the school's day to day business and smooth running.

.Location and Security procedures as above.

E Other Records- Creditors

Categories of Board of Management data:

The school may hold some or all of the following information about creditors (some of whom are self-employed individuals):

- name
- address
- contact details
- PPS number
- tax details

- bank details and
- amount paid

Purposes:

The purposes for keeping creditor records are:

This information is required for routine management and administration of the school's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners. Location and Security procedures as above.

F. Other Records: Charity Tax-back Forms

Categories of Board of Management data:

The school may hold the following data in relation to donors who have made charitable donations to the school:

- name
- address
- telephone number
- PPS number
- tax rate
- signature and
- the gross amount of the donation.

Purposes:

The purposes for keeping creditor records are:

Schools are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY2) and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. The information requested on the appropriate certificate is the parents' name, address, PPS number, tax rate, telephone number, signature and the gross amount of the donation. This is retained by the School in the event of audit by the Revenue Commissioners. Location and Security procedures as above.

CCTV Images/Recordings

CCTV is operational in St. Michael's School. A notice is displayed on entering the main school building. Images are only held for a maximum of 7 days and are then overwritten. Cameras are pointed and focused on key areas throughout the school and grounds.

Location of Cameras:

1. Foyer
2. Area at Senior Girls and Boys Toilet doors
3. Area at Junior Girls and Boys Toilet doors
4. Reception and Front Door area
5. Side door to the right of the Statue of Our Lady

6. Prayer Room Corridor
7. Three pathways at garden area adjacent to Cookery Kitchen / Prayer Room
8. Grass Area at exit door opposite St. John's class
9. Outside front of New Building
10. Dinner Room Corridor
11. Main Corridor at St. Mark's class
12. Main Corridor at St. Anthony's class
13. Main Corridor at St. Louise's class / Girls Senior Toilets
14. Corridor in New Building showing Fire Door
15. Corridor in New Building showing Toilet Doors
16. Steps entering the Yard and view of Gymnasium Door

These CCTV systems may record images of staff, students and members of the public who visit the premises. The viewing station is in the main school administration office.

Purposes:

Cameras are used to monitor activity within the school and grounds for the purpose of securing the safety of the school community and visitors.

Security: Access to images/recordings is restricted to the Principal, Deputy Principal & school secretary. It may be necessary for other staff members to view an image should a matter arise in line with our specified purpose above. Recordings are retained for 7 days and then over-written, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts legislation.

Examination Results

Categories: The school will hold data comprising examination results in respect of its pupils. These may include class, mid-term, annual, continuous assessment, standardised test results, diagnostic test results and /or State examinations.

Purposes: The main purpose for which these examination results and other records are held is to monitor a pupil's progress and to provide a sound basis for advising them and their parents or guardians about their education. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment, other schools to which pupils move and other similar bodies, e.g. QQI.

Location: In a secure, locked filing cabinet and in electronic format that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

Security: Paper Records are kept in a secure filing cabinet in a locked office. Computer records are kept on password protected PCs and cloud based storage is protected by up to date security and enhanced data protection and controlled password protected access to information, relevant to each staff member's role/duties.

Ownership

All records, regardless of format, created or received by staff in the course of their duties are the property of the school. (Primary Education Management Manual, August 2008).

Links to other policies and to curriculum delivery

Our school policies need to be consistent with one another, within the framework of the overall School Plan. Relevant school policies already in place or being developed or reviewed, shall be examined with reference to the *Data Protection Policy* and any implications which it has for them shall be addressed.

The following policies may be among those considered:

- Pupil Online Database (POD): Collection of the data for the purposes of complying with the Department of Education and Skills' pupil online database
- Child Safeguarding Statement & Risk Assessment
- Anti-Bullying Policy
- Code of Behaviour Policy and the addendum to the Code of Behaviour
- Covid-19 Response Plan
- Action Plan for Remote Learning
- Mobile Phone Policy
- Assessment Policy
- Critical Incident Policy
- Attendance Policy
- Admissions/Enrolment Policy
- Substance Use Policy
- ICT Acceptable Usage Policy
- Photographic Images Policy

Processing in line with data subject's rights

Data in this school will be processed in line with the data subject's rights. Data subjects have a right to:

- Know what personal data the school is keeping on them
- Request access to *any data* held about them by a data controller
- Prevent the processing of their data for direct-marketing purposes
- Ask to have inaccurate data amended
- Ask to have data erased once it is no longer necessary or irrelevant.

Data Processors

Where the school outsources to a data processor off-site, it is required by law to have a written contract in place. St. Michael's School's third party agreement specifies the conditions under which the data may be processed, the security conditions attaching to the processing of the data and that the data must be deleted or returned upon completion or termination of the contract.

Personal Data Breaches

All incidents in which personal data has been put at risk must be reported to the Office of the Data Protection Commissioner within 72 hours.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the BoM must communicate the personal data breach to the data subject without undue delay.

If a data processor becomes aware of a personal data breach, it must bring this to the attention of the data controller (BoM) without undue delay.

Dealing with a Data Access Request (DAR)

Individuals are entitled to a copy of their personal data on written request.

The individual is entitled to a copy of their personal data.

Request must be responded to within one month. An extension may be required e.g. over holiday periods.

No fee may be charged except in exceptional circumstances where the requests are repetitive or manifestly unfounded or excessive.

No personal data can be supplied relating to another individual apart from the data subject.

Providing information over the phone

An employee dealing with telephone enquiries should be careful about disclosing any personal information held by the school over the phone. In particular, the employee should:

- Ask that the caller put their request in writing
- Refer the request to the Principal for assistance in difficult situations
- Not feel forced into disclosing personal information.

Implementation Arrangements, Roles and Responsibilities

The Board of Management is the data controller and the Principal implements the Data Protection Policy, ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities. Staff are requested to avail of online training (PowerPoint presentation and video) provided by NABMSE. Further information on Data Protection in schools is brought to the attention of all staff and can be accessed on “gdpr4schools.ie”.

The following personnel have responsibility for implementing the Data Protection Policy:

Name	Responsibility
Board of management:	Data Controller
Principal:	Implementation of Policy
Teaching Staff	Awareness of responsibilities, confidentiality
Special Needs Assistants	Awareness of responsibilities, confidentiality
Bus Escorts	Awareness of responsibilities, confidentiality
Administrative personnel:	Security, confidentiality

Staff involved with IT:	Security, encryption, confidentiality
All Staff	Adherence to the Data Processing Principles
Entire School Community	Awareness and Respect for all Personal Data

Success Criteria

- Compliance with Data Protection Act and Statute of Limitations Act.
- Controlled, easy access to records.
- Framework in place for ease for compilation and reporting.
- Manageable storage of records.

Ratification & Communication

The updated Data Protection policy was ratified by the Board of Management on 17th February 2021. Secretary recorded the ratification in the Minutes of the meeting.

Monitoring the Implementation of the Policy

The implementation of the policy shall be monitored by the Principal and the Board of Management.

A copy of this policy will be made available to all staff as hard copy in the Policy folders, which are available in every classroom and on Aladdin to those who have access to same. A copy of this policy will be given to all bus escorts. It will be accessible to parents on the school website or a hard copy can be provided from the school office upon request.

Reviewing and Evaluating the Policy

The policy will be reviewed and evaluated after 2 years. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills or TUSLA), legislation and feedback from parents/guardians, students, school staff and others.

The policy will be revised as necessary in the light of such review and evaluation and within the framework of school planning during the normal operation of schools and during periods of remote learning.

Signed: *B. Bernadette Carron*

Chairperson, Board of Management

Date: Ratified *17th February 2021*

Appendix 1:  St. Michael's School Data Retention Periods for schools

<i>Pupil Related</i>	<i>Retention Periods</i>
School Register/Roll Books Enrolment Forms Disciplinary notes Test Results – Standardised Psychological Assessments etc. SEN Files/IEPS Accident Reports Child Protection Reports/Records S.29 Appeals	Indefinitely Hold until Pupil is 25 Years Never Destroy Hold until pupil is 25 Years Never Destroy Never Destroy Never Destroy Never Destroy Never Destroy
<i>Interview Records</i>	
Interview Board Marking Scheme Board of Management notes (for unsuccessful candidates)	18 months from close of competition plus 6 months in case Equality Tribunal needs to inform school that a claim is being taken
<i>Staff Records</i>	
Contract of Employment Teaching Council Registration Vetting Records Accident/Injury at work Reports	Retention for duration of employment + 7 years (6 years to make a claim against the school plus 1 year for proceedings to be served on school)
<i>BoM Records</i>	
BOM Agenda and Minutes CC V Recordings Payroll & Taxation Invoices/receipts Audited Accounts	Indefinitely 7 days normally. In the event of criminal investigation – as long as is necessary Revenue require a 6-year period after the end of the tax year Retain for 7 Years Indefinitely
<p><i>Why, in certain circumstances, does the Data Protection Commission recommend the holding of records until the former pupil has attained 25 years of age?</i></p> <p><i>The reasoning is that a pupil reaches the age of majority at 18 years and that there should be a 6-year limitation period in which it would be possible to take a claim against a school, plus 1 year for proceedings to be served on a school. The Statute of Limitations imposes a limit on a right of action so that after a prescribed period any action can be time barred.</i></p>	