



ST MICHAEL'S CATHOLIC COLLEGE PRIVACY NOTICE

Privacy Notice

St Michael's Catholic College is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your work relationship with us, in accordance with the General Data Protection Regulation (GDPR).

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

It applies to all current and former employees, workers and contractors.

Who Collects This Information

St Michael's Catholic College is a "data controller." This means that we are responsible for deciding how we hold and use personal information about you.

We are required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

The Categories of Information That We Collect, Process, Hold and Share

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, store and use the following categories of personal information about you: -

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;
- Emergency contact information such as your emergency contacts' names, relationships, phone numbers and email addresses;
- Information collected during the recruitment process that we retain during your employment including references, proof of right to work in the UK, application form, CV, qualifications;
- Employment contract information such as start dates, working hours, post, roles, workplace;
- Employment records such as job titles, work history, education and training details and professional memberships;
- Details of salary and benefits including payment details, payroll records, tax status information, national insurance number, pension and benefits information;
- Details of any dependants;
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;
- Information on grievances raised by or involving you;
- Information on conduct and/or other disciplinary issues involving you, including warnings issued to you;
- Details of your appraisals, performance reviews and capability issues;
- Details of your time and attendance records;
- Information about the use of our IT, communications and other systems, and other monitoring information;
- Details of your use of business-related social media;
- Images of staff captured by the College's CCTV system;
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions e.g. safeguarding within the College, you will be notified separately if this is to occur)
- Details in references about you that we give to others.
- Details of next of kin;
- Compensation history;
- A copy of the employee's driving licence;
- Teacher reference number;
- Annual leave details;
- Additional recruitment information to that already listed (e.g. copies of pre-vetting recruitment and identity checks; DBS checks etc);
- Photographs of employees.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information in your sickness, attendance and absence records such as number of absences, signing in/out of the college premises (e.g. for fire safety reasons) and reasons

(including sensitive personal information regarding your physical and/or mental health; information regarding time on statutory parental leave);

- Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs;
- Criminal records information as required by law to enable you to work with children;
- Your trade union membership;
- Genetic information and biometric data.

How We Collect This Information

We may collect this information from you, your personnel records, the Home Office, pension administrators, your doctors, from medical and occupational health professionals we engage, the DBS, your trade union, other employees, other professionals we may engage (e.g. to advise us generally), automated monitoring of our websites and other technical systems such as our computer networks and connections, college door entry/signing in systems collecting attendance data, catering system, copiers, CCTV and access control systems, remote access systems, email and instant messaging systems, intranet and internet facilities.

We will also collect additional personal information in the course of work-related activities throughout the period of you working for us.

How We Use Your Information

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances: -

- Where we need to perform the contract we have entered into with you;
- Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);
- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

- Where it is needed in the public interest or for official purposes;
- Where we need to protect your interests (or someone else's interests).

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests, provided your interests and fundamental rights do not override those interests. Please note that we may process your information without your knowledge or consent in compliance with the below rules, where this is required or permitted by law.

The situations in which we will process your personal information are listed below: -

- To determine recruitment and selection decisions on prospective employees;
- In order to carry out effective performance of the employees' contract of employment and to maintain employment records;

- To comply with regulatory requirements and good employment practice;
- To carry out vetting and screening of applicants and current staff in accordance with regulatory and legislative requirements;
- Enable the development of a comprehensive picture of the workforce and how it is deployed and managed;
- To enable management and planning of the workforce, including accounting and auditing;
- Personnel management including retention, sickness and attendance;
- Performance reviews, managing performance and determining performance requirements;
- In order to manage internal policy and procedure;
- Human resources administration including pensions, payroll and benefits;
- To determine qualifications for a particular job or task, including decisions about promotions;
- Evidence for possible disciplinary or grievance processes;
- Complying with legal obligations;
- To monitor and manage staff access to our systems and facilities in order to protect our networks, the personal data of our employees and for the purposes of safeguarding;
- To monitor and protect the security of our network and information, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution;
- Education, training and development activities;
- To monitor compliance with equal opportunities legislation;
- To answer questions from insurers in respect of any insurance policies which relate to you;
- Determinations about continued employment or engagement;
- Arrangements for the termination of the working relationship;
- Dealing with post-termination arrangements;
- Health and safety obligations;
- Prevention and detection of fraud or other criminal offences; and
- To defend the College in respect of any investigation or court proceedings and to comply with any court or tribunal order for disclosure.
- Further information is available by emailing St Michael's Catholic College using contact details from <https://www.stmichaelscollege.org.uk/>.
- Determining the terms on which you work for us;
- Checking you are legally entitled to work in the UK;
- Checking the award of Qualified Teacher Status, completion of teacher induction and prohibitions, sanctions and restrictions that might prevent the individual from taking part in certain activities or working in specific positions via the Teacher Services Online platform;
- To maintain our single central record and to comply with our general safeguarding obligations
- To provide information on our website about our employees
- Where appropriate, to disclose certain information in the Academy's accounts in accordance with the ESFA's Academies Financial Handbook and Accounts direction
- Liaising with your pension provider
- Administering contracts of employment

- In order to operate as a school, which may involve us sharing certain information about our staff with our stakeholders or processing correspondence or other documents, audits or reports which contain your personal data
- Responding to complaints or investigations from stakeholders or our regulators
- Providing references to prospective employers
- Education, training and development requirements
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work
- Ascertaining your fitness to work
- To conduct data analytics studies to review and better understand employee retention and attrition rates
- In connection with the Transfer of Undertaking (Protection of Employment) Regulations 2006, for example, if a service is outsourced or in connection with an academy conversion.
- To maintain and promote equality in the workplace
- To comply with requirements of the Archdiocese of Southwark to share personal data about employees to the extent that they require it to fulfil their functions – further details are available on the Archdiocese’s privacy notice, available here: [insert link]
- To receive advice from external advisors and consultants
- In appropriate circumstances to liaise with regulatory bodies, such as the NCTL, the Department for Education, the Teachers Regulation Agency, the DBS and the Local Authority about your suitability to work in a school or in connection with other regulatory matters.

In addition, the College also uses CCTV camera around the College site for security purposes and for the protection of staff and pupils. CCTV footage may be referred to during the course of disciplinary procedures (for staff and pupils) or to investigate other issues. CCTV footage involving staff will only be processed to the extent that it is lawful to do so. Please see out CCTV policy for more detail.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

How We Use Particularly Sensitive Information

“Special categories” of particularly sensitive personal information require higher levels of protection and further justification for collecting, storing and using this type of personal information. We may process this data in the following circumstances: -

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring (or in relation to our pension scheme);
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is necessary to protect your interests (or someone else’s interests) and you are not capable of giving your consent, or where you have already made the information public.

Situations in which we will use your sensitive personal information

In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment. On rare occasions, there may be other reasons for processing, such as it is in the public interest to do so.

We will use this information in the following ways: -

- Collecting information relating to leave of absence including the reasons for the leave, which may include sickness absence or family related leave;
- To comply with employment and other laws;
- Collecting information about your physical or mental health, or disability status, to ensure your health and welfare in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to manage sickness absence and to administer benefits;
- Collecting information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- Collecting information about your religious beliefs ensure your suitability to hold certain posts within the College.
- To record trade union membership information to pay trade union premiums and to comply with employment law obligations.

Do we need your consent?

We do not need your consent if we use your particularly sensitive information in accordance with our written policy where processing is necessary:

- to carry out our legal obligations or exercise specific rights in the field of employment law;
- for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to

data protection and we provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

In other circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract of employment with us that you agree to any request for consent from us.

Criminal Convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about criminal convictions, for example, if information about criminal convictions comes to light as a result of our recruitment and Disclosure and Barring Service checks, or if information about criminal convictions comes to light during your employment with us.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of working for us.

Automated Decision Making

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision making in the following circumstances: -

- Where we have notified you of the decision and given you 21 days to request a reconsideration;
- Where it is necessary to perform the contract with you and appropriate measures are put in place to safeguard your rights; or
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Sharing Data

We may need to share your data with third parties, including third party service providers and other organisations where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. These include the following: -

- the Department for Education (DfE);
- Ofsted;
- Prospective Employers;
- Welfare services (such as social services);
- Law enforcement officials such as police, HMRC;
- LADO;
- Training providers;
- Professional advisors such as lawyers and consultants;
- Support services (including HR support, insurance, IT support, information security, pensions and payroll);
- The Local Authority;
- Occupational Health;
- DBS; and
- Recruitment and supply agencies.
- The Education & Skills Funding Agency;
- The Archdiocese of Southwark;
- The Teaching Regulation Agency;
- The Teacher's Pension Service;
- The Local Government Pension Scheme which is administered by the Local Pension fund Authority;
- Insurance providers / the Risk Protection Arrangement.

Information will be provided to those agencies securely or anonymised where possible. The recipient of the information will be bound by confidentiality obligations, we require them to respect the security of your data and to treat it in accordance with the law. Some of the organisations referred to above are joint data controllers. This means we are all responsible to you for how we process your data.

We may transfer your personal information outside the UK and the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

Why might we share your personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you, where it is needed in the public interest or for official purposes, or where we have your consent.

Which third-party service providers process your personal information?

“Third Parties” includes third-party service providers (including contractors and designated agents). The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, IT services.

Department for Education

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information about our staff with the Department for Education (DfE) under regulation 7 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 as amended.

Department for Education data collection requirements

The following is information provided by the DfE concerning the reason it collects data about school employees:

- The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.
- To find out more about the data collection requirements placed on us by the DfE including the data that we share with them, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

The DfE may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff by:

- conducting research or analysis;
- producing statistics; and/or
- providing information, advice or guidance

The DfE has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data.

To be granted access to school workforce information, organisations must comply with the DfE’s strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the DfE’s data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

To contact the department, please visit: <https://www.gov.uk/contact-dfe>

How secure is your information with third-party service providers?

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

What about other third parties?

We may share your personal information with other third parties, for example if there was a TUPE transfer of staff in future. We may also need to share your personal information with a regulator or to otherwise comply with the law.

From time to time, we may disclose your personal data in response to a request for information pursuant to the Freedom of Information Act 2000 or following a data subject access request. We may approach you for your consent but, in any event, we will only disclose your personal data if we are satisfied that it is reasonable to do so in all the circumstances. This means that we may refuse to disclose some or all of your personal data following receipt of such a request.

Transferring information outside the UK and the EU

Wherever possible we do not transfer your personal data outside the UK or to an international organisation.

There might occasions where processing of your personal data may sometimes involve a transfer of data outside the UK.

- Whenever we transfer your personal data out of the UK, we ensure a similar degree of protection is afforded to it by ensuring we will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data.
- Where we use certain service providers, we may use specific contracts approved for use in the UK which give personal data the same protection it has in the UK.

We may sometimes transfer your personal data outside of the UK if, for example, we are arranging a school trip and we are booking transport, accommodation or activities. In these circumstances, we will obtain your consent for us to process your data in this way.

Retention Periods

Except as otherwise permitted or required by applicable law or regulation, the College only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes. Details of retention periods for different aspects of your personal information are available in our Data Retention Policy which is available from <https://www.stmichaelscollege.org.uk/wp-content/uploads/2019/11/St-Michaels-Catholic->

[College-Data-Protection-Policy-GDPR-2018-20-New-policy-which-now-includes-data-retention-data-breach-FOI-Social-media-CCTV-Electro.pdf](#)

To determine the appropriate retention period for personal data, the College considers the amount, nature, and sensitivity of personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for processing the personal data, whether we can fulfil the purposes of processing by other means and any applicable legal requirements. The College typically retains personal data for 6 years subject to any exceptional circumstances or to comply with laws or regulations that require a specific retention period.

Please refer to the College's Data Retention Policy for further details.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy.

Security

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way, altered or disclosed). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. Details of these measures will be available from the College's Information Security Policy.

Third parties who are processing personal data on our behalf will only process your personal information on our instructions and where they have agreed to treat information confidentially and to keep it secure.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Your Rights of Access, Correction, Erasure and Restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances by law you have the right to: -

- Access your personal information (commonly known as a "subject access request"). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However we may charge a reasonable fee if your request for access is manifestly unfounded or excessive. Alternatively we may refuse to comply with the request in such circumstances.

- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You have the right to object where we are processing your personal information for direct marketing purposes.
- Transfer your personal information to another party.

If you want to exercise any of the above rights, please contact St Michael's Catholic College in writing.

The legal timescales for the school / trust to respond to a Subject Access Request is one calendar month. As the school/trust has limited staff resources outside of term time, we encourage governor / trustees / staff / pupils / parents and carers to submit Subject Access Requests during term time and to avoid sending a request during periods when the School is closed or is about to close for the holidays where possible. This will assist us in responding to your request as promptly as possible. For further information about how we handle Subject Access Requests, please see our Data Protection Policy.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to Withdraw Consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Principal in writing St Michael's Catholic College via contact@stmichaelscollege.org.uk. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

How to Raise a Concern

We hope that St Michael's Catholic College can resolve any query you raise about our use of your information in the first instance.

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information, then you can contact the DPO on the details below: -

Data Protection Officer Name: Craig Stilwell
Data Protection Officer Details: Judicium Consulting Ltd
72 Cannon Street
London
EC4N 6AE
Data Protection Officer Email: dataservices@judicium.com
Data Protection Officer Phone: 0203 326 9174

You have the right to make a complaint at any time to the Information Commissioner’s Office, the UK supervisory authority for data protection issues.

You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF

Changes to This Privacy Notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact the Principal in writing St Michael’s Catholic College via contact@stmichaelscollege.org.uk.

I, _____ (name), acknowledge that on _____ (date), I received a copy of St Michael’s Catholic College privacy notice and I have read and understood it.

Signed:..... **Date:**.....