ST MICHAEL'S CATHOLIC COLLEGE
DATA PROTECTION POLICY 2018-2020

Introduction

The General Data Protection Regulation (GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The College will protect and maintain a balance between data protection rights in accordance with the GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the College and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the College's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

SECTION 1 - DEFINITIONS

Personal data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special Category Data

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

Data Subject

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

Data Controller

The organisation storing and controlling such information (i.e. the College) is referred to as the Data Controller.

Processing

Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Automated Processing

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

Data Protection Impact Assessment (DPIA)

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

Criminal Records Information

This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

SECTION 2 - WHEN CAN THE COLLEGE PROCESS PERSONAL DATA

Data Protection Principles

The College are responsible for and adhere to the principles relating to the processing of personal data as set out in the GDPR.

The principles the College must adhere to are: -

(1) Personal data must be processed lawfully, fairly and in a transparent manner;

(2) Personal data must be collected only for specified, explicit and legitimate purposes;

(3) Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

(4) Personal data must be accurate and, where necessary, kept up to date;

(5) Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed; and

(6) Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Further details on each of the above principles is set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

The College only collect, process and share personal data fairly and lawfully and for specified purposes. The College must have a specified purpose for processing personal data and special category of data as set out in the GDPR.

Before the processing starts for the first time we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Personal Data

The College may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;

- For the purposes of the College's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

The College may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the College in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing in necessary for archiving, statistical or research purposes.

The College identifies and documents the legal grounds being relied upon for each processing activity.

Consent

Where the College relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the College will normally seek another legal basis to process that data. However if explicit consent is required the data subject will be provided with full information in order to provide explicit consent.

The College will keep records of consents obtained in order to demonstrate compliance with consent requirements under the GDPR.

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

The College will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

The College will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the College shall delete or anonymise the data. Please refer to the College's Data Retention Policy for further guidance.

Principle 4: Personal data must be accurate and, where necessary, kept up to date

The College will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the College.

Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The College will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the College's Data Retention Policy for further details about how the College retains and removes data.

Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

In order to assure the protection of all data being processed, the College will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -

- Encryption;
- Pseudonymisation (this is where the College replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The College follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The College will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

Full details on the College's security measures are set out in the College's Information Security Policy.

Sharing Personal Data

The College will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party: -

- Has a need to know the information for the purposes of providing the contracted services;
- Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract that contains GDPR approved third party clauses has been obtained.

There may be circumstances where the College is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the local authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our College shall be clearly defined within written notifications and details and basis for sharing that data given.

Transfer of Data Outside the European Economic Area (EEA)

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

The College will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the GDPR. All staff must comply with the College's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

SECTION 3 - DATA SUBJECT'S RIGHTS AND REQUESTS

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the College handle their personal data are set out below: -

(a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;

(b) Receive certain information about the College's processing activities;

(c) Request access to their personal data that we hold;

(d) Prevent our use of their personal data for marketing purposes;

(e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

(f) Restrict processing in specific circumstances;

(g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) Request a copy of an agreement under which personal data is transferred outside of the EEA;

(i) Object to decisions based solely on automated processing;

(j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;

(k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(l) Make a complaint to the supervisory authority; and

(m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the College to verify the identity of the individual making the request.

Subject Access Requests

A Data Subject has the right to be informed by the College of the following: -

(a) Confirmation that their data is being processed;

(b) Access to their personal data;

(c) A description of the information that is being processed;

(d) The purpose for which the information is being processed;

(e) The recipients/class of recipients to whom that information is or may be disclosed;

(f) Details of the College's sources of information obtained;

(g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct.

(h) Other supplementary information

Any Data Subject who wishes to obtain the above information must notify the College in writing of his or her request. This is known as a Data Subject Access Request.

The request should in the first instance be sent to Mr J. Arda, Assistant Principal in charge of Data.

Direct Marketing

The College are subject to certain rules and privacy laws when marketing. For example a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The College will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The College will promptly respond to any individual objection to direct marketing.

Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the College in the course of their employment or engagement. If so, the College expects those employees to help meet the College's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example by complying with rules on access to College premises, computer access, password protection and secure file storage and destruction. (Please refer to the College's Information Security Policy for further details about our security processes);
- Not to remove personal data or devices containing personal data from the College premises unless appropriate security measures are in place (such as Pseudonymisation, encryption, password protection) to secure the information;
- Not to store personal information on local drives.

SECTION 4 - ACCOUNTABILITY

The College will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the GDPR principles.

The College have taken the following steps to ensure and document GDPR compliance: -

Data Protection Officer (DPO)

Please find below details of the College's Data Protection Officer: -

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

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances: -

(a) If you are unsure of the lawful basis being relied on by the College to process personal data;

(b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);

(c) If you need to draft privacy notices or fair processing notices;

(d) If you are unsure about the retention periods for the personal data being processed but would refer you to the College's data retention policy in the first instance;

(e) If you are unsure about what security measures need to be put in place to protect personal data;

(f) If there has been a personal data breach and would refer you to the procedure set out in the College's breach notification policy;

(g) If you are unsure on what basis to transfer personal data outside the EEA;

(h) If you need any assistance dealing with any rights invoked by a data subject;

(i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;

(j) If you plan to undertake any activities involving automated processing or automated decision making;

(k) If you need help complying with applicable law when carrying out direct marketing activities;

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

Personal Data Breaches

The GDPR requires the College to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches (Mr J. Arda at St Michael's Catholic College) or the DPO (who is Craig Stilwell).

Transparency and Privacy Notices

The College will provide detailed, specific information to data subjects. This information will be provided through the College's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices sets out information for data subjects about how the College use their data and the College's privacy notices are tailored to suit the data subject.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the GDPR including the identity of the data protection officer, the College's contact details, how and why we will use, process, disclose, protect and retain personal data.

When personal data is collected indirectly (for example from a third party or publically available source), we will provide the data subject with the above information as soon as

possible after receiving the data. The College will also confirm whether that third party has collected and processed data in accordance with the GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the GDPR

Privacy by Design

The College adopt a privacy be design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the College takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the College conduct DPIAs for any new technologies or programmes being used by the College which could affect the processing of personal data. In any event the College carries out DPIAs when required by the GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data;
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

Record Keeping

The College is required to keep full and accurate records of our data processing activities. These records include: -

- The name and contact details of the College;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;

- Details of the College's processing activities and purposes;
- Details of any third-party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

Training

The College will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

Audit

The College through its data protection officer regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

Related Policies

Staff should refer to the following policies that are related to this data protection policy in the appendices below: -

- Appendix A – Data retention policy;
- Appendix B – Data breach policy;
- Appendix C – Freedom of information policy;
- Appendix D – Social media policy;
- Appendix – Information security policy (in progress);
- CCTV policy (in progress).

These policies are also designed to protect personal data and along with privacy notices can be found at https://www.stmichaelscollege.org.uk/gdpr/.

Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the College.

Appendix A

ST MICHAEL'S CATHOLIC COLLEGE
DATA RETENTION POLICY 2018

The School has a responsibility to maintain its records and record keeping systems. When doing this, the School will take account of the following factors: -

- The most efficient and effective way of storing records and information;
- The confidential nature of the records and information stored;
- The security of the record systems used;
- Privacy and disclosure; and
- Their accessibility.

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It does, however, reflect the School's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the School from time to time and any changes will be notified to employees within one month of the date on which the change is intended to take effect. The School may also vary any parts of this procedure, including any time limits, as appropriate in any case.

DATA PROTECTION

This policy sets out how long employment-related and pupil data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of the School. The School's Data Protection Policy outlines its duties and obligations under the GDPR.

RETENTION SCHEDULE

Information (hard copy and electronic) will be retained for at least the period specified in the attached retention schedule. When managing records, the School will adhere to the standard retention times listed within that schedule.

Paper records will be regularly monitored by Mrs S. Shaw, Head of Administration.

Electronic records will be regularly monitored by:

Pupil files	Mrs S. Shaw, Head of Administration
Safeguarding	Ms J. Nottage, Assistant Principal – Inclusion and Behaviour
Academic info	Mr R. Richards, Data Manager
	Ms P. Lynch, Examinations Officer and 6th Form Secretary
HR	Mrs V. Ferguson, PA to the Principal
Finance	Ms A. Pasvani, Business Manager
Parent information	Mrs S. Shaw, Head of Administration
Governance	Ms S. Dosseter, Clerk to the Governors
IT	Mr N. Haxby

In addition, it is expected for relevant members of the Senior Leadership Team, Heads of Department, Leaders of Learning and any other postholders who utilise data in line with their roles to retain academic or pastoral information for the periods as appropriate to the Retention Policy.
The schedule is a relatively lengthy document listing the many types of records used by the school and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements.

DESTRUCTION OF RECORDS

Where records have been identified for destruction they should be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

All paper records containing personal information, or sensitive policy information should be shredded before disposal where possible. All other paper records should be disposed of by an appropriate waste paper merchant. All electronic information will be deleted.

The School maintains a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record in this list at least: -

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

ARCHIVING

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives is maintained by Mrs V. Ferguson, PA to the Principal and Mrs S. Shaw, Head of Administration. The appropriate staff member, when archiving documents should record in this list the following information: -

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

TRANSFERRING INFORMATION TO OTHER MEDIA

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media or virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.

RESPONSIBILITY AND MONITORING

Mr J. Arda, as Assistant Principal in charge of Data, has primary and day-to-day responsibility for implementing this Policy. The Data Protection Officer, in conjunction with the School is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation. The data protection officer will consider the suitability and adequacy of this policy and report improvements directly to management.

Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records.

Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this Policy and are given adequate and regular training on it.

RETENTION SCHEDULE

FILE DESCRIPTION	RETENTION PERIOD
Employment Records	
Job applications and interview records of unsuccessful candidates	12 months after notifying unsuccessful candidates, unless the school has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained
Job applications and interview records of successful candidates	6 years after employment ceases
Written particulars of employment, contracts of employment and changes to terms and conditions	6 years after employment ceases
Right to work documentation including identification documents	2 years after employment ceases
Immigration checks	Two years after the termination of employment
DBS checks and disclosures of criminal records forms	As soon as practicable after the check has been completed and the outcome recorded (i.e. whether it is satisfactory or not) unless in exceptional circumstances (for example to allow for consideration and resolution of any disputes or complaints) in which case, for no longer than 6 months.
Change of personal details notifications	No longer than 6 months after receiving this notification
Emergency contact details	Destroyed on termination
Personnel and training records	While employment continues and up to six years after employment ceases
Annual leave records	Six years after the end of tax year they relate to or possibly longer if leave can be carried over from year to year
Consents for the processing of personal and sensitive data	For as long as the data is being processed and up to 6 years afterwards
Working Time Regulations: • Opt out forms • Records of compliance with WTR	• Two years from the date on which they were entered into • Two years after the relevant period

Disciplinary and training records	6 years after employment ceases
Allegations of a child protection nature against a member of staff including where the allegation is founded	10 years from the date of the allegation or the person's normal retirement age (whichever is longer). This should be kept under review. Malicious allegations should be removed.
Financial and Payroll Records	
Pension records	15 years
Retirement benefits schemes – notifiable events (for example, relating to incapacity)	6 years from the end of the scheme year in which the event took place
Payroll and wage records	6 years after end of tax year they relate to
Maternity/Adoption/Paternity Leave records	3 years after end of tax year they relate to
Statutory Sick Pay	3 years after the end of the tax year they relate to
Current bank details	No longer than necessary
Agreements and Administration Paperwork	
Collective workforce agreements and past agreements that could affect present employees	Permanently
Trade union agreements	10 years after ceasing to be effective
School Development Plans	5 years from the life of the plan
Professional Development Plans	6 years from the life of the plan
Visitors Book and Signing In Sheets	6 years
Newsletters and circulars to staff, parents and pupils	2 years
Health and Safety Records	
Health and Safety consultations	Permanently
Health and Safety Risk Assessments	3 years from the life of the risk assessment
Any reportable accident, death or injury in connection with work	For at least twelve years from the date the report was made
Accident reporting	Adults – 6 years from the date of the incident Children – when the child attains 25 years of age.

Fire precaution log books	6 years
Medical records and details of: - • control of lead at work • employees exposed to asbestos dust • records specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry made in the record
Records of tests and examinations of control systems and protection equipment under COSHH	5 years from the date on which the record was made
Temporary and Casual Workers	
Records relating to hours worked and payments made to workers	3 years
Pupil Records	
Admissions records	2 years from the date of admission
Admissions register	Entries to be preserved for three years from date of entry
School Meals Registers	3 years
Free School Meals Registers	6 years
Pupil Record	This may include: Information received from the feeder Primary school Exclusion letters, if appropriate Holiday requests Additional educational needs The above list is not exhaustive due to unique matters that arise in the individual case of each pupil. Currently pupil records are archived securely at the College in case information needs to be made available concerning any present or past student at St Michael's.
Attendance Registers	3 years from the date of entry
Special Educational Needs files, reviews and individual education plans (this includes any	Until the child turns 25.

statement and all advice and information shared regarding educational needs)	
Emails	
Other Records	
The above list is not exhaustive due to matters arising. The policy will be updated to reflect any changes, as and when appropriate.	

Appendix B

ST MICHAEL'S CATHOLIC COLLEGE
DATA BREACH POLICY 2018

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the School of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

Definitions

Personal Data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special Category Data

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Data Subject

Person to whom the personal data relates.

ICO

ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

Responsibility

Mr J. Arda, Assistant Principal in charge of Data, has overall responsibility for breach notification within the School. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

In the absence of the Assistant Principal in charge of Data, please do contact Ms F. Corcoran, Principal.

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this policy or the GDPR or if you have any concerns that this policy is not being or has not been followed.

The DPO's contact details are set out below: -

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

Security and Data-Related Policies

Staff should refer to the following policies that are related to this data protection policy: - Security Policy which sets out the School's guidelines and processes on keeping personal data secure against loss and misuse.

Data Protection Policy which sets out the School's obligations under GDPR about how they process personal data.

These policies are also designed to protect personal data and can be found at https://www.stmichaelscollege.org.uk/gdpr/.

Data Breach Procedure

What Is A Personal Data Breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

When Does It Need To Be Reported?

The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

Reporting A Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should: -

- Complete a data breach report form (which can be obtained from Mr J Arda j.arda@stmichaelscollege.org.uk);
- Email the completed form to Mr J.Arda.

Where appropriate, you should liaise with your line manager about completion of the data report form. Breach reporting is encouraged throughout the School and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, Mr J.Arda or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. Mr J.Arda will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DPO.

Managing and Recording The Breach

On being notified of a suspected personal data breach, Mr J.Arda will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:-

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the School's data breach register;
- Notify the ICO;
- Notify data subjects affected by the breach;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

Notifying the ICO

Craig Stilwell will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (I.e. it is not 72 working hours). If the School are unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, Mr J.Arda will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures the School have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, Mr J.Arda will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example by making a statement on the School website).

Notifying Other Authorities

The School will need to consider whether other parties need to be notified of the breach. For example: -

- Insurers;
- Parents;
- Third parties (for example when they are also affected by the breach);
- Local authority;
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

Assessing the Breach

Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);

- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

Preventing Future Breaches

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will: -

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether its necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to Mr J.Arda or the DPO. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the College.

Appendix C

ST MICHAEL'S CATHOLIC COLLEGE
FREEDOM OF INFORMATION POLICY 2018

Introduction

The Freedom of Information Act 2000 gives individuals the right to access official information from public bodies. Under the Act, any person has a legal right to ask for access to information held by the College. They are entitled to be told whether the College holds the information, and to receive a copy, subject to certain exemptions. While the Act assumes openness, it recognises that certain information is sensitive. There are exemptions to protect this information.

Public Authorities should be clear and proactive about the information they will make public. For this reason, a publication scheme is available (See Appendix A).

This policy does not form part of any individual's terms and conditions of employment with the College and is not intended to have contractual effect.

This policy should be used in conjunction with the College's Internet Use Policy and Data Protection Policy.

Requests

Requests under Freedom of Information should be made to Mr J. Arda, Assistant Principal in charge of Data. However the request can be addressed to anyone in the College; so all staff need to be aware of the process for dealing with requests.

Requests for information that are not data protection or environmental information requests will be covered by the Freedom of Information Act: -

Data Protection enquiries (or subject access requests) are requests where the enquirer asks to see what personal information the College holds about the enquirer. If the enquiry is a Data Protection request, the College's Data Protection Policy should be followed.

Environmental Information Regulations enquiries are those which relate to air, water, land, natural sites, built environment, flora and fauna, and health, and any decisions and activities affecting any of these. These could therefore include enquiries about recycling, phone masts, College playing fields, car parking etc. If the enquiry is about environmental information,

follow the guidance on the Department for Environment, Food and Rural Affairs (DEFRA) website.

Freedom of Information requests must be made in writing, (including email), and should include the enquirers name and correspondence address (email addresses are allowed), and state what information they require. There must be enough information in the request to be able to identify and locate the information. If this information is covered by one of the other pieces of legislation (as referred to above), they will be dealt with under the relevant policy/procedure related to that request.

If the request is ambiguous and/or the College require further information in order to deal with your request, the College will request this further information directly from the individual making the request. Please note that the College do not have to deal with the request until the further information is received. Therefore, the time limit starts from the date that the College receives all information required in order to deal with the request.

The requester does not have to mention the Act, nor do they have to say why they want the information. There is a duty to respond to all requests, telling the enquirer whether or not the information is held, and supplying any information that is held, except where exemptions apply. There is a time limit of 20 working days excluding school holidays for responding to the request.

Information

Provided all requirements are met for a valid request to be made, the College will provide the information that it holds (unless an exemption applies).

"Holding" information means information relating to the business of the College:

- That the College has created; or
- That the College has received from another body or person; or
- Held by another body on the College's behalf.

Information means both hard copy and digital information, including email.

If the information is held by another public authority, such as the Local Authority, first check with them they hold it, then transfer the request to them. If this applies, the College will notify the enquirer that they do not hold the information and to whom they have transferred the request. The College will continue to answer any parts of the enquiry in respect of information it does hold.

When the College does not hold the information, it has no duty to create or acquire it; just to answer the enquiry, although a reasonable search will be made before confirming whether the College has the information requested.

If the information requested is already in the public domain, for instance through the Publication Scheme or on the St Michael's Catholic College website, the College will direct the enquirer to the information and explain how to access it.

The requester has the right to be told if the information requested is held by the College (subject to any of the exemptions). This obligation is known as the College's "duty to confirm or deny" that it holds the information. However, the College does not have to confirm or deny if:-

- The exemption is an absolute exemption; or
- In the case of qualified exemptions, confirming or denying would itself disclose exempted information.

Vexatious Requests

There is no obligation on the College to comply with vexatious requests. A vexatious request is one which is designed to cause inconvenience, harassment or expense rather than to obtain information, and would require a substantial diversion of resources or would otherwise undermine the work of the College. This however does not provide an excuse for bad records management.

In addition, the College do not have to comply with repeated identical or substantially similar requests from the same applicant unless a "reasonable" interval has elapsed between requests.

Fees

The College may charge the requester a fee for providing the requested information. This will be dependent on whether the staffing costs in complying with the request exceeds the "threshold." The threshold is currently £450 with staff costs calculated at a fixed rate of £25 per hour (therefore 18 hours' work is required before the threshold is reached).

If a request would cost less than the threshold, then the College can only charge for the cost of informing the applicant whether the information is held, and communicating the information to the applicant (e.g. photocopying, printing and postage costs).

When calculating costs/threshold, the College can take account of the staff costs/time in determining whether the information is held by the College, locating and retrieving the information, and extracting the information from other documents. The College will not take account of the costs involved with considering whether information is exempt under the Act.

If a request would cost more than the appropriate limit, (£450) the College can turn the request down, answer and charge a fee or answer and waive the fee.

If the College are going to charge they will send the enquirer a fees notice. The College do not have to comply with the request until the fee has been paid. More details on fees can be found on the ICO website.

If planning to turn down a request for cost reasons, or charge a high fee, you should contact the applicant in advance to discuss whether they would prefer the scope of the request to be modified so that, for example, it would cost less than the appropriate limit.

Where two or more requests are made to the College by different people who appear to be acting together or as part of a campaign the estimated cost of complying with any of the requests may be taken to be the estimated total cost of complying with them all.

Time Limits

Compliance with a request must be prompt and within the time limit of 20 working days (excluding school holidays). Failure to comply could result in a complaint by the requester to the Information Commissioner. The response time starts from the time the request is received.

Where the College has asked the enquirer for more information to enable it to answer, the 20 working days start time begins when this further information has been received.

If some information is exempt this will be detailed in the College's response.

If a qualified exemption applies and the College need more time to consider the public interest test, the College will reply in 20 working days (term time only) stating that an exemption applies but include an estimate of the date by which a decision on the public interest test will be made. This should be within a "reasonable" time.

Where the College has notified the enquirer that a charge is to be made, the time period stops until payment is received.

Third Party Data

Consultation of third parties may be required if their interests could be affected by release of the information requested, and any such consultation may influence the decision.

Consultation will be necessary where:

- Disclosure of information may affect the legal rights of a third party, such as the right to have certain information treated in confidence or rights under Article 8 of the European Convention on Human Rights;
- The views of the third party may assist the College to determine if information is exempt from disclosure; or
- The views of the third party may assist the College to determine the public interest test.

Personal information requested by third parties is also exempt under this policy where release of that information would breach the Data Protection Act. If a request is made for a document (e.g. Governing Body minutes) which contains personal information whose release to a third party would breach the Data Protection Act, the document may be issued by blanking out the relevant personal information as set out in the redaction procedure.

Exemptions

The presumption of the Freedom of Information Act is that the College will disclose information unless the Act provides a specific reason to withhold it. The Act recognises the need to preserve confidentiality and protect sensitive material in certain circumstances.

The College may refuse all/part of a request, if one of the following applies: -

1) There is an exemption to disclosure within the act;
2) The information sought is not held;
3) The request is considered vexatious or repeated; or
4) The cost of compliance exceeds the threshold.

A series of exemptions are set out in the Act which allow the withholding of information in relation to an enquiry. Some are very specialised in their application (such as national security) and would not usually be relevant to schools.

There are two general categories of exemptions:-

1) **Absolute**: where there is no requirement to confirm or deny that the information is held, disclose the information or consider the public interest; and
2) **Qualified**: where, even if an exemption applies, there is a duty to consider the public interest in disclosing information.

Absolute Exemptions

There are eight absolute exemptions set out in the Act. However, the following are the only absolute exemptions which will apply to the College: -

- Information accessible to the enquirer by other means (for example by way of the College's Publication Scheme);
- National Security/Court Records;
- Personal information (i.e. information which would be covered by the Data Protection Act);
- Information provided in confidence.

If an absolute exemption exists, it means that disclosure is not required by the Act. However, a decision could be taken to ignore the exemption and release the information taking into account all the facts of the case if it is felt necessary to do so.

Qualified Exemptions

If one of the below exemptions apply (i.e. a qualified disclosure), there is also a duty to consider the public interest in confirming or denying that the information exists and in disclosing information.

The qualified exemptions under the Act which would be applicable to the College are: -

- Information requested is intended for future publication (and it is reasonable in all the circumstances for the requester to wait until such time that the information is actually published);
- Reasons of National Security;
- Government/International Relations;
- Release of the information is likely to prejudice any actual or potential legal action or formal investigation involving the College;
- Law enforcement (i.e. if disclosure would prejudice the prevention or detection of crime, the prosecution of offenders or the administration of justice);
- Release of the information would prejudice the ability of the College to carry out an effective audit of its accounts, resources and functions;
- For Health and Safety purposes;
- Information requested is Environmental information;
- Information requested is subject to Legal professional privilege; and
- For "Commercial Interest" reasons.

Where the potential exemption is a qualified exemption, the College will consider the public interest test to identify if the public interest in applying the exemption outweighs the public interest in disclosing it.

In all cases, before writing to the enquirer, the person given responsibility by the College for dealing with the request will need to ensure that the case has been properly considered, and that the reasons for refusal, or public interest test refusal, are sound.

Refusal

If it is decided to refuse a request, the College will send a refusals notice, which must contain

- The fact that the responsible person cannot provide the information asked for;
- Which exemption(s) apply;
- Why the exemption(s) apply to this enquiry (if it is not self-evident);
- Reasons for refusal; and
- The College's complaints procedure.

For monitoring purposes and in case of an appeal against a decision not to release the information or an investigation by the Information Commissioner, the responsible person must keep a record of all enquiries where all or part of the requested information is withheld and exemptions are claimed. The record must include the reasons for the decision to withhold the information.

Complaints/Appeals

Any written (including email) expression of dissatisfaction should be handled through the College's existing complaints procedure. Wherever practicable the review should be handled by someone not involved in the original decision.

The Governing Body should set and publish a target time for determining complaints and information on the success rate in meeting the target. The College should maintain records of all complaints and their outcome.

If the outcome is that the College's original decision or action is upheld, then the applicant can appeal to the Information Commissioner. The appeal can be made via their website or in writing to:

Customer Contact
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

Appendix

1. ST MICHAEL'S CATHOLIC COLLEGE

St Michael's Catholic College is an 'Outstanding School' with a flourishing Teaching School.

2. INTRODUCTION – STATUS OF THE SCHEME

2.1 This publication scheme has been prepared in accordance with the provisions of the Freedom of Information Act 2000 (FOI) and comply with the model publication scheme prepared and approved by the Information Commissioner.

2.2 This publication scheme commits St Michael's Catholic College to make information available to the public as part of its normal business activities. The information covered by the scheme is included in the classes of information referred to below, where this information is held by the College.

2.3 St Michael's will:

Proactively publish or otherwise routinely make available, information which it holds, including environmental information, which falls within the classifications below.

- Specify the information that is held by St Michael's and falls within the classifications below.
- Proactively publish or otherwise routinely make available, information in line with the statements contained within this scheme.
- Publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- Review and regularly update the information made available under this scheme.
- Produce and publish a schedule of any fees that it may charge for access to information which is made proactively available under this scheme.
- Make this publication scheme available to the public.
- Publish any dataset held by the college that has been requested, and any updated versions it holds, unless the college is satisfied that it is not appropriate to do so; to publish the dataset, where reasonably practicable, in an electronic form that is capable of re-use; and, if any information in the dataset is a relevant copyright work and St Michael's is the only owner, to make the information available for re-use under a specified licence. The term 'dataset' is defined in section 11(5) of the Freedom of Information Act. The terms 'relevant copyright work' and specified licence' are defined in section 19(8) of

that Act.

3. CLASSES OF INFORMATION

3.1 Who we are and what we do

Organisational information, locations and contacts, constitutional and legal governance.

3.2 What we spend and how we spend it

Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.

3.3 What our priorities are and how we are doing

Strategy and performance information, plans, assessments, inspections and reviews.

3.4 How we make decisions

Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.

3.5 Our policies and procedures

Current written protocols for delivering our functions and responsibilities.

3.6 Lists and registers

Information held in registers required by law and other lists and registers relating to the functions of the authority.

3.7 The services we offer

Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

3.8 The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

4. THE METHOD BY WHICH INFORMATION PUBLISHED UNDER THIS SCHEME WILL BE MADE AVAILABLE

4.1 St Michael's will indicate clearly to the public what information is covered by this scheme and how it can be obtained.

4.2 All statutory policies and the majority of key information that the public may require is accessible via the college web site.

4.3 Where it is within the capability of St Michael's the information will be provided on our website. Where it is impracticable to make information available on a website, or when an individual does not wish to access the information by a website, the college will indicate how information can be obtained by other means and will provide it by those means.

4.4 In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

4.5 Information will be provided in the language in which it is held or in such other language that is legally required. Where St Michael's is legally required to translate any information, it will do so.

4.6 Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

5. CHARGES WHICH MAY BE MADE FOR INFORMATION PUBLISHED UNDER THIS SCHEME

5.1 The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by St Michael's for routinely published material will be justified and transparent and kept to a minimum.

5.2 Material which is published and accessed on a website will be provided free of charge. Charges may be made for information subject to a charging regime specified by Parliament.

5.3 Charges may be made for actual disbursements incurred such as:

- Photocopying
- Postage and packaging
- The costs directly incurred as a result of viewing information

5.4 Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance

with a published schedule or schedules of fees which is readily available to the public.

5.5 Charges may also be made for making datasets (or parts of datasets) that are relevant copyright works available for re-use. These charges will be in accordance with either regulations made under section 11B of the Freedom of Information Act or other enactments.

5.6 If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.

6. Written Requests

Information held by a public authority that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.

Annex 1: GUIDE TO INFORMATION AVAILABLE FROM ST MICHAEL'S CATHOLIC COLLEGE UNDER THE PUBLICATION SCHEME

INFORMATION TO BE PUBLISHED	HOW THE INFORMATION CAN BE OBTAINED	COST
Class 1 – Who we are and what we do		
Members of St Michael's Board and their appointments	College website	No charge
Articles of Association	Hard copy	No charge
Contact details for St Michael's Catholic College	College website	No charge
Corporate details: registered office; directors; members; registered office	Companies House website -www.companieshouse.gov.uk	Companies House charges
Staffing structure	Hard copy	Schedule of charges
Class 2 – What we spend and how we spend it		
Statutory accounts	Published on College website each year	No charge
Procurement – policy and opportunities	College website	No charge
Pay policy	Hard copy	Schedule of charges
Class 3 What are our priorities and how are we doing		
Plans for future development	College website	No charge
Achievements	College website	No charge
Exam results	College website	No charge
Latest Ofsted reports	College website	No charge
Newsletters	College website	No charge
Class 4 How we make decisions		
Scheme of delegation	Hard copy	Schedule of charges
Agendas of meetings of the Board of St Michael's Catholic College and its Committees	Hard copy	Schedule of charges
Minutes of meetings of the Board of St Michael's Catholic College and its Committees – this will exclude information that is regarded as confidential	Hard copy	Schedule of charges
Information to be published	**How the information can be obtained**	**Cost**
Admissions procedures	Academy website	No charge
Class 5 Our policies and Procedures		
Policies and procedures including:		
Safeguarding policies and procedures	Academy website	No charge
Health & Safety Policy	Academy website	No charge
Complaints procedure	Academy website	No charge
Equality and Diversity policies	Academy website	No charge
Home Academy Agreement	Hard copy	No charge
Health and Sex Education policies	Academy website	No charge
Class 6 List and Registers		
Any lists and registers that the Federation is required to keep	Hard copy	Schedule of charges
Class 7 The services we offer		
Prospectuses	Hard copy	No charge
Out of hours clubs	Academy website	No charge
Extra curricular activities	Academy website	No charge

Schedule of charges

TYPE OF CHARGE	COST	BASIS OF CHARGE
Photocopying	**20p per page black and white A4**	
	35p per page colour A4	
	45p per page A3	

Publication Scheme under the
Freedom of Information Act 2000 ("FOIA 2000") 2017

Appendix D

ST MICHAEL'S CATHOLIC COLLEGE
SOCIAL MEDIA POLICY 2018

Introduction

This policy applies to all College staff regardless of their employment status. It is to be read in conjunction with the College's ICT Policy. This policy does not form part of the terms and conditions of employee's employment with the College and is not intended to have contractual effect. It does however set out the College's current practices and required standards of conduct and all staff are required to comply with its contents. Breach of the provisions of this policy will be treated as a disciplinary offence which may result in disciplinary action up to and including summary dismissal in accordance with the College's Disciplinary Policy and Procedure.

This Policy may be amended from time to time and staff will be notified of any changes no later than one month from the date those changes are intended to take effect.

Purpose of this Policy

The College recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, LinkedIn, blogs and Wikipedia. However, staff use of social media can pose risks to the College's confidential and proprietary information, its reputation and it can jeopardise our compliance with our legal obligations.

To minimise these risks, avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate work related purposes, all College staff are required to comply with the provisions in this policy.

Who is covered by this policy?

This policy covers all individuals working at all levels and grades within the College, including senior managers, officers, governors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as **Staff** in this policy).
Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

Scope and Purpose of this Policy

This policy deals with the use of all forms of social media including Facebook, LinkedIn, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs.

It applies to the use of social media for both work and personal purposes, whether during work hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.

Breach of this policy may result in disciplinary action up to and including dismissal.
Disciplinary action may be taken regardless of whether the breach is committed during working hours and regardless of whether the College's equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Personnel responsible for implementing the policy

The Board of Governors have overall responsibility for the effective operation of this policy, but have delegated day-to-day responsibility for its operation to the Principal.

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Principal in liaison with the IT Development Manager.

All senior College Staff have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All College Staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Principal in the first instance. Questions regarding the content or application of this policy should be directed by email to Mr J. Arda, Assistant Principal in charge of Data on j.arda@stmichaelscollege.org.uk.

Compliance with related policies and agreements

Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

a) Breach our Electronic information and communications systems policy;
b) Breach our obligations with respect to the rules of relevant regulatory bodies;
c) Breach any obligations they may have relating to confidentiality;
d) Breach our Disciplinary Rules;
e) defame or disparage the College, its Staff, its pupils or parents, its affiliates, partners, suppliers, vendors or other stakeholders;
f) Harass or bully other Staff in any way or breach our Anti-harassment and bullying policy;
g) Unlawfully discriminate against other Staff or third parties or breach our Equal opportunities policy;
h) Breach our Data protection policy (for example, never disclose personal information about a colleague online);
i) Breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).
j)

Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the College and create legal liability for both the author of the reference and the organisation.

Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

Personal use of social media

Personal use of social media is never permitted during working time or by means of our computers, networks and other IT resources and communications systems.
Staff should not use a work email address to sign up to any social media and any personal social media page should not make reference to their employment with the College (excluding LinkedIn or simillar, where prior permission is sought from Mr J. Arda, Assistant Principal in charge of Data).

Staff must not take photos or posts from social media that belongs to the College for their own personal use.

Monitoring

The contents of our IT resources and communications systems are the College's property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

The College reserves the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your acknowledgement of this policy and your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The College may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.
All Staff are advised not to use our IT resources and communications systems for any matter that he or she wishes to be kept private or confidential from the College.

Educational or Extra Curricular Use of Social Media

If your duties require you to speak on behalf of the College in a social media environment, you must follow the protocol outlined below.

The Principal may require you to undergo training before you use social media on behalf of the College and impose certain requirements and restrictions with regard to your activities.
Likewise, if you are contacted for comments about the College for publication anywhere, including in any social media outlet, you must direct the inquiry to the Principal and must not respond without advanced written approval.

Recruitment

The College may use internet searches to perform pre-employment checks on candidates in the course of recruitment. Where the College does this, it will act in accordance with its data protection and equal opportunities obligations.

Responsible use of social media

The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

Photographs for use of Social Media

Any photos for social media posts may only be taken using College cameras/devices or devices that have been approved in advance by Mr J. Arda, Assistant Principal in charge of Data). Where any device is used that does not belong to the College all photos must be deleted immediately from the device, once the photos have been uploaded to a device belonging to the College.

Staff Protocol for use of Social Media

Where any post is going to be made on the College's own social media the following steps must be taken:

1. Ensure that permission from the child's parent has been sought before information is used on social media (in writing from the parent), if relevant.
2. Ensure that there is no identifying information relating to a child/children in the post - for example any certificates in photos are blank/without names or the child's name cannot be seen on the piece of work.
3. The post must be a positive and relevant post relating to the children, the good work of staff, the College or any achievements.
4. Social Media can also be used to issue updates or reminders to parents/guardians and St Michael's Catholic College will have overall responsibility for this. Should you wish for any reminders to be issued you should contact Mr J. Arda by email to ensure that any post can be issued.
5. The proposed post must be presented to Mr J. Arda for confirmation that the post can 'go live' before it is posted on any social media site.
6. Staff can post the information, but must have responsibility to ensure that the Social Media Policy has been adhered to.
7.

Protecting our business reputation

Staff must not post disparaging or defamatory statements about:

i. The College;
ii. Current, past or prospective Staff as defined in this policy
iii. Current, past or prospective pupils
iv. Parents, carers or families of (iii)
v. The College's suppliers and services providers; and
vi. Other affiliates and stakeholders.

Staff should also avoid social media communications that might be misconstrued in a way that could damage the College's reputation, even indirectly.

If Staff are using social media they should make it clear in any social media postings that they are speaking on their own behalf. Staff should write in the first person and use a personal rather than College e-mail address when communicating via social media.

Staff are personally responsible for what they communicate in social media. Staff should remember that what they publish might be available to be read by the masses (including the College itself, future employers and social acquaintances) for a long time. Staff should keep this in mind before they post content.

If Staff disclose whether directly or indirectly their affiliation to the College as a member of Staff whether past, current or prospective, they must also state that their views do not represent those of the College.

Staff must ensure that their profile and any content posted are consistent with the professional image they are required to present to colleagues, pupils and parents.

Staff must avoid posting comments about confidential or sensitive College related topics. Even if Staff make it clear that their views on such topics do not represent those of the College, such comments could still damage the College's reputation and incur potential liability.

If a member of Staff is uncertain or concerned about the appropriateness of any statement or posting, he or she should refrain from making the communication until he or she has discussed it with his Line Manager or Head of Department.

If a member of Staff sees content in social media that disparages or reflects poorly on the College, it's Staff, pupils, parents, service providers or stakeholders, he or she is required to report this in the first instance to the Head Teacher without unreasonable delay. All staff are responsible for protecting the College's reputation.

Respecting intellectual property and confidential information

Staff should not do anything to jeopardise College confidential information and intellectual property through the use of social media.

In addition, Staff should avoid misappropriating or infringing the intellectual property of other College's, organisations, companies and individuals, which can create liability for the College, as well as the individual author.

Staff must not use the College's logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without express prior written permission from the Principal.

To protect yourself and the College against liability for copyright infringement, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Principal in the first instance before making the communication.

Respecting colleagues, pupils, parents, clients, service providers and stakeholders

Staff must not post anything that their colleagues, the College's past, current or prospective pupils, parents, service providers or stakeholders may find offensive, including discriminatory comments, insults or obscenity.

Staff must not post anything related to colleagues, the College's past, current or prospective pupils, parents, service providers or stakeholders without their advanced written permission.

Monitoring and review of this policy

Mr J. Arda, Assistant Principal in charge of Data together with Ms F. Corcoran, Principal shall be responsible for reviewing this policy from time to time to ensure that it meets legal requirements and reflects best practice. The Board of Governors has responsibility for approving any amendments prior to implementation.

The Principal has responsibility for ensuring that any person who may be involved with administration or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.

If Staff have any questions about this policy or suggestions for additions that they would like to be considered on review, they may do so by emailing Mr J. Arda, Assistant Principal in charge of Data) in the first instance.

Appendix E

ST MICHAEL'S CATHOLIC COLLEGE
PRIVACY NOTICE – STAFF 2018

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).

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

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 names, relationship, 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, hours worked, post, roles;
- Education and training details;
- 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 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);
- 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;
- Information on grievances raised by or involving you;
- Information on conduct and/or other disciplinary issues involving 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.
-

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.
-

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 needed in the public interest or for official purposes;
- 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 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. Please note that we may process your information without your knowledge or consent, where this is require 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/.

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 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).

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

Sensitive personal information (as defined under the GDPR as "special category data") 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.

We will use this information in the following ways: -

- Collecting information relating to leave of absence, 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.
- To record trade union membership information to pay trade union premiums and to comply with employment law obligations.

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. 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.

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.

Sharing Data

We may need to share your data with third parties, including third party service providers 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.

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.

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

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.

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.

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). 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 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

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
.
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 clearly 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.
- 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.
- To object to processing in certain circumstances (for example for direct marketing purposes).
- To 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.

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 which cannot be resolved by St Michael's Catholic College, 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

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. Please contact the Principal in writing St Michael's Catholic College via contact@stmichaelscollege.org.uk.

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.

Appendix F

ST MICHAEL'S CATHOLIC COLLEGE
PRIVACY NOTICE – PUPILS AND PARENTS 2018

Privacy Notice

St Michael's Catholic College is committed to protecting the privacy and security of personal information. This privacy notice describes how we collect and use personal information about pupils, in accordance with the General Data Protection Regulation (GDPR), section 537A of the Education Act 1996 and section 83 of the Children Act 1989.

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 pupils.

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

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

- Personal information such as name, pupil number, date of birth, gender and contact information;
- Emergency contact and family lifestyle information such as names, relationship, phone numbers and email addresses;
- Characteristics (such as ethnicity, language, nationality, religion, country of birth and free school meal eligibility);
- Attendance details (such as sessions attended, number of absences and reasons for absence);
- Financial details;
- Post 16 learning information;
- Performance and assessment information;
- Behavioural information (including exclusions);
- Special educational needs information;
- Relevant medical information;
- Special categories of personal data (including ethnicity, relevant medical information, special educational needs information, dietary requirements, accident reports, etc.);
- Images of pupils engaging in school activities, and images captured by the School's CCTV system;
- Information about the use of our IT, communications and other systems, and other monitoring information;
- Electronic identification data collected through cookies from the College website which uses Google analytics. Please refer to the College's Cookie Policy for further details.

Collecting This Information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

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.

How We Use Your Personal Information

We hold pupil data and use it for: -

- Pupil selection (and to confirm the identity of prospective pupils and their parents);
- Providing education services and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs;
- Informing decisions such as the funding of schools;
- Assessing performance and to set targets for schools;
- Safeguarding pupils' welfare and providing appropriate pastoral (and where necessary medical) care;
- Support teaching and learning;
- Giving and receive information and references about past, current and prospective pupils, and to provide references to potential employers of past pupils;
- Managing internal policy and procedure;
- Enabling pupils to take part in assessments, to publish the results of examinations and to record pupil achievements;
- To carry out statistical analysis for diversity purposes;
- Legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with legal obligations and duties of care;
- Enabling relevant authorities to monitor the school's performance and to intervene or assist with incidents as appropriate;
- Monitoring use of the school's IT and communications systems in accordance with the school's IT security policy;
- Making use of photographic images of pupils in school publications, on the school website and on social media channels;
- Security purposes, including CCTV; and
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

The Lawful Basis on Which We Use This Information

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

- Consent: the individual has given clear consent to process their personal data for a specific purpose;
- Contract: the processing is necessary for a contract with the individual;
- Legal obligation: the processing is necessary to comply with the law (not including contractual obligations);
- Vital interests: the processing is necessary to protect someone’s life.
- Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law; and

- The Education Act 1996: for Departmental Censuses 3 times a year. More information can be found at: https://www.gov.uk/education/data-collection-and-censuses-for-schools.

We need all the categories of information in the list above primarily to allow us to comply with legal obligations. Please note that we may process information without knowledge or consent, where this is require or permitted by law.

Sharing Data

We may need to share your data with third parties where it is necessary. There are strict controls on who can see your information. We will not share your data if you have advised us that you do not want it shared unless it's the only way we can make sure you stay safe and healthy or we are legally required to do so.

We share pupil information with: -

- the Department for Education (DfE) - on a statutory basis under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013;
- Ofsted;
- Other Schools that pupils have attended/will attend;
- NHS;
- Welfare services (such as social services);
- Law enforcement officials such as police, HMRC;
- Local Authority Designated Officer;
- Professional advisors such as lawyers and consultants;
- Support services (including insurance, IT support, third party software to support College services e.g. Show My Homework, Parent Pay, etc); and
- The Local Authority.

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.

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

Why We Share This Information

We do not share information about our pupils with anyone without consent unless otherwise required by law.

For example, we share student's data with the DfE on a statutory basis which underpins school funding and educational attainment. To find out more about the data collection requirements placed on us by the DfE please go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Storing Pupil Data

The School keep information about pupils on computer systems and sometimes on paper.

Except as required by law, the School only retains information about pupils for as long as necessary in accordance with timeframes imposed by law and our internal policy.

If you require further information about our retention periods, please refer to our Data Retention Policy which is available from: https://www.stmichaelscollege.org.uk/gdpr/.

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 limited circumstances.

Pupils will not be subject to automated decision-making, unless we have a lawful basis for doing so and we have notified you.

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).

The National Pupil Database

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to

https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

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

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases 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 store and handle the data

To be granted access to pupil information, organisations must comply with 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 department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting Access to Your Personal Data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, contact St Michael's Catholic College.

You also have the right to: -

- Object to processing of personal data that is likely to cause, or is causing, damage or distress;
- Prevent processing for the purposes of direct marketing;
- Object to decisions being taken by automated means;
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- Claim compensation for damages caused by a breach of the data protection regulations.

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

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 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 St Michael's Catholic College. 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.

Contact

If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you raise your concern with St Michael's Catholic College 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 which cannot be resolved by St Michael's Catholic College, 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

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 at https://ico.org.uk/concerns.

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.

Appendix G

Address of the College: St Michael's Catholic College, Llewellyn Street, Bermondsey, London SE16 4UN

Name and contact details of designated contact within the School:
J Arda, Assistant Principal – Data, Telephone number: 020 7237 6432
Email address: j.arda@stmichaelscollege.org.uk

Name and contact details of Data Protection Officer:
Craig Stilwell, Judicium Consulting Ltd. Telephone number: 0203 326 9174.
Email address: dataservices@judicium.com

Date of Report:

Summary Of The Breach
Data Type And Individuals Affected
Effects Of The Breach
Actions Taken
Data Protection Measures In Place
Any Other Relevant Information/Status
Status

July 2018

Date Ratified by the Governors: ……

Signed: ……...

Review Date: September 2020

ST MICHAEL'S CATHOLIC COLLEGE
CCTV POLICY 2019

Introduction

The school recognises that CCTV systems can be privacy intrusive.
Review of this policy shall be repeated regularly and whenever new equipment is introduced a review will be conducted and a risk assessment put in place. We aim to conduct reviews no later than every two years.

Objectives

The purpose of the CCTV system is to assist the school in reaching these objectives:

(a) To protect pupils, staff and visitors against harm to their person and/or property.
(b) To increase a sense of personal safety and reduce the fear of crime.
(c) To protect the school buildings and assets.
(d) To support the police in preventing and detecting crime.
(e) To assist in identifying, apprehending and prosecuting offenders.
(f) To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence
(g) To assist in managing the school.

Purpose of This Policy

The purpose of this Policy is to regulate the management, operation and use of the CCTV system (closed circuit television) at the school.

Statement of Intent

Notification has been submitted to the Information Commissioner and the next renewal date has been recorded.

The CCTV system will aim to comply with the requirements both of the Data Protection Act and the most recent Commissioner's Code of Practice.

The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site and make clear who is responsible for the equipment.

Recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated. In the absence of compelling a need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than 30 days. If used for an incident they will be deleted August of each year (confirm with FCO) unless there are other exemptions that apply.

System Management

Access to the CCTV system and data shall be password protected.

The CCTV system will be administered and managed by Mr N Haxby, ICT Development Manager who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager the system will be managed by J Arda, Assistant Principal.

The system and the data collected will only be available to the Systems Manager, his/her replacement and appropriate members of the senior leadership team as determined by the Principal.

The CCTV system is designed to be in continuous operation throughout the year, though the school does not guarantee that it will be working during these hours.

The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional.

Cameras have been selected and positioned so as to provide clear, usable images in strategic positions.

Where a person other than those mentioned in paragraph 5.3 above, requests access to the CCTV data or system, the System Manager must satisfy him/herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists access will be refused.

Details of all visits and visitors will be recorded in InVentry including time/data of access and details of images viewed and the purpose for so doing. This has been in place since 1st July 2019.

Downloading Captured Data onto Other Media

In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any download media used to record events from the hard drive must be prepared in accordance with the following procedures: -

(a) Each stored media clip must be identified by a unique mark.

(b) The System Manager has arranged for the timestamping of the date and time of each stored media clip, including its reference using cloud storage.

(c) Media clips required for evidential purposes must be secured by the System Manager, then dated and stored in a separate secure evidence cloud drive. Media gathered for the police would follow police procedure for submitting evidence.

Complaints About the Use Of CCTV

Any complaints in relation to the school's CCTV system should be addressed to the Principal.

Request for Access by The Data Subject

The Data Protection Act provides Data Subjects – those whose image has been captured by the CCTV system and can be identified - with a right to data held about themselves, including those obtained by CCTV. Requests for such data should be made to Mr J. Arda, Assistant Principal in charge of Data.

Public Information

Copies of this policy will be available to the public from the school office.

July 2019

Date Ratified by the Governors: ……

Signed: ……...

Review Date: September 2020

ST MICHAEL'S CATHOLIC COLLEGE
ELECTRONIC INFORMATION AND COMMUNICATIONS SYSTEMS POLICY 2019

Introduction

The College's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service.

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of staff at the College who are required to familiarise themselves and comply with its contents. The College reserves the right to amend its content at any time.

This policy outlines the standards that the College requires all users of these systems to observe, the circumstances in which the College will monitor use of these systems and the action the College will take in respect of any breaches of these standards.

The use by staff and monitoring by the College of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the General Data Protection Regulation (GDPR) and all data protection laws and guidance in force.

Staff are referred to the College's Data Protection Policy for further information. The College is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect the College's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the College's disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

The College has the right to monitor all aspects of its systems, including data which is stored under the College's computer systems in compliance with the GDPR.

This policy mainly deals with the use (or misuse) of computer equipment, e-mail, internet connection, telephones, iPads (and other smart or mobile devices), and voicemail, but it applies equally to the use of fax machines, copiers, scanners, and the like.

Equipment Security and passwords

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.
Passwords are unique to each user and staff are required to select a password that cannot be easily broken and which contains at least 8 characters including numbers, and letters and special characters. There will

be a change on 26th of August 2019 for teaching and support staff to have complex rules implemented: 8 characters minimum, including at least one letter, one numeric, one capital and one special character.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with Mr N. Haxby, ICT Development Manager as appropriate and necessary. No staff passwords will be stored. They will be reset, if appropriate. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the College's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If given access to the College e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off or lock their screens when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Team and/or Mr N. Haxby, ICT Development Manager may do spot checks from time to time to ensure compliance with this requirement.

Staff should be aware that if they fail to log off and leave their terminals unattended, they may be held responsible for another user's activities on their terminal in breach of this policy, the College's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Logging off prevents another member of staff accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that he or she was not the party responsible.

Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of Mr N. Haxby, ICT Development Manager.

On the termination of employment for any reason, staff are required to provide a full handover detailing the drives, folders and files where their work can be located and accessed. The College reserves the right to require employees to hand over all College data held in computer useable format including their ID card and any other digital devices.

Members of staff who have been issued with a laptop, tablet (or other computer or mobile device) must ensure that it is kept secure at all times, especially when travelling during any commute or on College business. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g. ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers.

Systems Use and Data Security

Members of staff should not delete, destroy or modify any of the College's existing systems, programs, information or data which could have the effect of harming or exposing to risk or harm the College, its staff, students, or any other party.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from Mr N. Haxby, ICT Development Manager who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

Where consent is given all files and data should always be virus checked before they are downloaded onto the College's systems. If in doubt, the employee should seek advice from Mr N. Haxby, ICT Development Manager or a member of the Senior Leadership Team. Downloading illegal media / software and/or watching illegal streaming services is in breach of the Acceptable Use of IT Policy.

No device or equipment should be attached to our systems without the prior approval of Mr N. Haxby, ICT Development Manager or Senior Leadership Team. This includes, but is not limited to, any digital device or telephone, iPad (or other mobile device tablet), USB device, i-pod, digital camera, MP3 player, infra-red connection device, BYOD WiFi access and USB storage. This list is not exhaustive and will be updated as technology changes.

Staff should be cautious when opening e-mails from unknown or suspicious sources, under no circumstances should unexpected attachments be opened without first checking with NHA. Mr N. Haxby, ICT Development Manager should be informed immediately if a suspicious attachment / suspected virus is received. The College reserves the right to block access to attachments to e-mail for the purpose of effective use of the system and compliance with this policy. The College also reserves the right not to transmit any e-mail message.

Staff should not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

Misuse of the College's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled Inappropriate Use of the College's Systems and guidance under "E-mail etiquette and content" below.

E-mail etiquette and content

E-mail is a vital business tool, but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline within the scope of the Acceptable Use of IT Policy.

Staff are permitted to make incidental personal use of the College's e-mail facility provided such use is in strict accordance with this policy (see Personal Use below). Excessive or inappropriate personal use of the College's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

Staff should always consider if e-mail is the appropriate medium for a particular communication. The College encourages all members of staff to make direct contact with individuals rather than communicate by e-mail wherever possible to maintain and enhance good working relationships.

All electronic communications to parents/external organisations should be done in a professional manner. All members of staff should remember that e-mails can be the subject of legal action for example in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff who sent them and the College. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the College in the same way as the contents of letters or faxes.

Staff should ensure that they access their e-mails regularly at appropriate points within the working day. Staff should endeavour to respond to internal e-mails marked 'high priority' as soon as is reasonably practicable.

If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via e-mail, you should refer to the St Michael's Catholic College Disciplinary policy 2019-20 for further information and guidance.

As general guidance, staff must not:

Send any e-mail, including resending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally;

- Send any e-mail communication which may be regarded as harassing or insulting. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis in accordance with normal and courteous practice;
- Send or forward private e-mails at work which they would not want a third party to read;
- Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the College;
- Agree to terms, enter into contractual commitments or make representations by e-mail unless the appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter;
- Download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- Send messages containing any reference to other individuals or any other business that may be construed as libellous;
- Send messages from another worker's computer or under an assumed name unless specifically authorised;
- Send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure;
- E-mail may normally only be used to communicate internally with colleagues and students (where appropriate and necessary) and externally to parents, suppliers and third parties on academic/service related issues. Urgent or important messages to family and friends are permitted, but must be of a serious nature;

The College recognises that it is not always possible to control incoming mail. Any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive should be deleted at once. Any member of staff who finds that they are receiving such communications from known sources is responsible for contacting that source in order to request that such communication is not repeated and reported to your line manager or senior member of staff.

Staff who receive an e-mail which has been wrongly delivered should, where possible, contact the sender of the message. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or forwarded to another member of staff or used in any way. J Arda, Assistant Principal, should be informed as soon as reasonably practicable.

<u>Use of the web and the internet</u>

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the College, especially if a member of staff has accessed, downloaded, stored or forwarded inappropriate material from the website.
Staff must not therefore access from the College's system any web page or any files (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition. Viewed content needs to be appropriate for use in the College, if

the website is hijacked / redirects to inappropriate link inform N. Haxby, ICT Development Manager, so it can be blocked.

Any confidential data contained on College IT systems may not be copied without appropriate permissions from a member of the senior leadership team.

The College reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers that personal use is excessive or otherwise in breach of this policy.

Inappropriate use of equipment and systems

Incidental use of personal devices is permissible provided it is in full compliance with the College's rules, policies and procedures. Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the College's Disciplinary Policy. Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.
Where evidence of misuse is found the College may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary such information may be handed to the police in connection with a criminal investigation.

July 2019

Date Ratified by the Governors: ……

Signed: ……...

Review Date: September 2020

ST MICHAEL'S CATHOLIC COLLEGE
INFORMATION SECURITY POLICY 2019

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The College is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by the College to achieve this, including to: -

- protect against potential breaches of confidentiality;
- ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- increase awareness and understanding at the College of the requirements of information security and the responsibility to staff to protect the confidentiality and integrity of the information that they themselves handle.

Introduction

Information Security can be defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.
Staff are referred to the College's Data Protection Policy, Data Breach Policy and Electronic Information and Communication Systems Policy for further information. These policies are also designed to protect personal data and can be found at https://www.stmichaelscollege.org.uk/gdpr/.
For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks and smartphones.

Scope

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the College, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.
This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.
All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the College's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the College and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

General principles

All data stored on our IT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information. Further details on the categories of data can be

found in the College's Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with Mr N Haxby, ICT Development Manager the appropriate security arrangements for the type of information they access in the course of their work.

All data stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by Mr N Haxby, ICT Development Manager or by such third party/parties as he may authorise.

All staff are collectively responsible for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data). Matters are overseen by Mr N Haxby, ICT Development Manager unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to Mr J Arda, Assistant Principal who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found from: https://www.stmichaelscollege.org.uk/gdpr/).

Physical security and procedures

Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows. At the end of the working day, or when you leave your desk unoccupied, all such paper documents shall be securely locked away to avoid unauthorised access.

Available storage rooms, locked cabinets, and other storage systems with locks shall be used to store paper records when not in use as well classroom or office doors being shut to prevent unauthorised access.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of College.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform Mr N Haxby as soon as possible. Increased risks of vandalism and or burglary shall be considered when assessing the level of security required.

The College carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.

The College has an intercom system to minimise the risk of unauthorised people from entering the College premises.
The College closes the College gates during certain hours to prevent unauthorised access to the building.

An alarm system is set nightly.

Visitors should be required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information. Visitors should also sign in using the InVentry system upon entering and leaving the College site.

Computers and IT

Responsibilities of Mr N Haxby, ICT Development Manager

Mr N Haxby, ICT Development Manager shall be responsible for the following:

a) ensuring that all IT Systems are reviewed, along with Mr J Arda, and are fit for purpose to meet the College's security requirements;
b) supporting that all members of staff are aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the GDPR and the Computer Misuse Act 1990 and to inform Mr J Arda, who is the SLT link overseeing the relevant policies and procedures
c) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;
d) ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;
e) receiving and handling all reports relating to IT Security matters and taking appropriate action in response including, in the event that any reports relate to personal data, informing the Data Protection Officer;
f) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at each respective College building.

Responsibilities – Members of staff

All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

You must immediately inform Mr J Arda, Assistant Principal of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Breach Notification Policy.

Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to Mr N Haxby, ICT Development Manager immediately.

You are not entitled to install any software of your own without the approval of Mr N Haxby, ICT Development Manager and may only be installed where that installation poses no security risk and would not breach any software licence agreements.

Prior to installation of any software onto the IT Systems, you must obtain written permission by Mr N Haxby and/or Mr J Arda. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.

Prior to any usage of physical media (e.g. USB memory sticks or disks of any kind) for transferring files, you must make sure to have the physical media is virus-scanned. If you detect any virus this must be reported immediately to Mr N Haxby, ICT Development Manager (this rule shall apply even where the anti-virus software automatically fixes the problem).

Access security

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

The College has a secure firewall and anti-virus software in place. These reduce the risk of unauthorised access and to protect the College's network. The College also informs individuals about e-safety to ensure everyone is aware of how to protect the College's network and themselves.

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT Department.

Computers and other electronic devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this this time period or disable the lock.

All mobile devices provided by the College, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the College's Data Protection Policy (GDPR) and/or the requirement for confidentiality in respect of certain information.

Data security

Personal data sent over the College network will be otherwise secured. All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from Mr N Haxby, ICT Development Manager who will consider bona fide requests for work purposes.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the College's Wi-Fi provided that you follow the ICT Development Manager's requirements and instructions governing this use. All usage of your own device(s) whilst connected to the College's network or any other part of the IT Systems is subject to all relevant College Policies (including, but not limited to, this policy). Mr N Haxby, ICT Development Manager may at any time request the immediate disconnection of any such devices without notice.

Electronic storage of data

All portable data, and in particular personal data, should be stored on encrypted drives or secure methods such as the use of Google Drive.

All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

You should not store any sensitive personal data on any mobile device, whether such device belongs to the College or otherwise without prior written approval of the Principal. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the College's computer network or cloud in order for it to be backed up.
All electronic data stored on the network must be securely backed up by the end of the each working day and is done by Mr N Haxby, ICT Development Manager.

Home working

You should not take confidential or other information home without prior permission of Mr J Arda, Assistant Principal, and only do so where satisfied appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.
When you have been given permission to take confidential or other information home, you must ensure that:

a) the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
b) all confidential material that requires disposal is shredded or, in the case of electronical material, securely destroyed, as soon as any need for its retention has passed.

Communications, transfer, internet and email use

When using the College's IT Systems, you are subject to and must comply with the College's Electronic Information and Communication Systems Policy.

The College works to ensure the systems do protect pupils and staff and are reviewed and improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to Mrs D Freegard, Designated Safeguarding Lead.

Appropriate checks are made to ensure that filtering methods are purposeful, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the College cannot accept liability for the material accessed or its consequence.

All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email, secure cloud or sent by tracked DX (document exchange) or recorded delivery. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

Postal, DX, fax and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

You should be careful about maintaining confidentiality when speaking in public places. For example, if discussing sensitive personal data pertaining to a student, member of staff or member of the wider school community, office or classroom doors should be closed.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the College.

Personal or confidential information should not be removed from the College without prior permission from the Principal except where the removal is temporary and necessary. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

a) not transported in see-through or other un-secured bags or cases;
b) not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
c) not left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.)

Reporting security breaches

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to Mr J Arda, Assistant Principal. All members of staff have an obligation to report actual or potential data protection compliance failures.

When receiving a question or notification of a breach, Mr J Arda, Assistant Principal shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the Mr J Arda, Assistant Principal. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, Mr J Arda, Assistant Principal.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to Mr J Arda, Assistant Principal.

All IT security breaches shall be fully documented.

Full details on how to notify of data breaches are set out in the Breach Notification Policy.

Related Policies

Staff should refer to the following policies that are related to this information security policy:

- Electronic information and communication systems policy;
- Data breach policy;
- Data protection Policy.

July 2019

Date Ratified by the Governors: ……

Signed: ……...

Review Date: September 2020