ST MICHAEL'S CATHOLIC COLLEGE
INFORMATION TECHNOLOGY POLICY 2024-25 incl. Online Safety Policy-Acceptable use of IT Policy for Staff, Governors & Visitors INCL. the Biometrics Policy & Cookies

1. Aim

As part of the curriculum entitlement, students study computing across the key stages. This comprises three main strands: digital literacy, computer science and information technology. It is the latter and its use at St Michael's Catholic College that provides the focus in this policy.

Given the rapid advance of technology in today's society, we hope all pupils can:

- Understand and apply the fundamental principles of computing
- Analyse problems in computational terms, gain practical experience of writing computer programs
- Evaluate, apply and be creative with information technology, including new or emerging technologies using IT confidently and responsibly within the College and beyond the College day

We will support this by:

- Ensuring all pupils reach the highest possible levels of achievement
- Enabling pupils to become independent users of IT, and benefit from the IT resources, tools and its impact on society
- Teaching pupils how to be safe and to learn good practice in the use of Technology for Learning

IT includes any hardware or software for users to electronically communicate or handle data or information.

Management responsible for the computing and IT strategy

Mr Arda	Assistant Principal, Technology for Learning and UK GDPR
Mr Haxby	IT Manager
Mr Clarke	Head of ICT and Computing

Scope:

- Enhancing curricular experiences to enhance teaching and learning and further develop IT capability
- Updating policies and schemes of work
- Ordering and updating resources and advising on their use
- Providing or organising training so that all staff are confident IT practitioners
- Updating SLT and governors about IT strategies
- Contributing to the SIP and SEF at regular points (at least annually)
- Liaising effectively with RM, the College's Managed Service

Health and Safety

All activities, whether in College or off site, will be guided by the College's Health and Safety, Online Safety policies and government guidance, as appropriate. Where necessary, individual UK Data Protection Impact Assessments (DPIAs) will be put into place to ensure the safety of pupils and the integrity of the College IT system. All equipment is PAT tested annually.

'Online Safety' refers to all technologies and electronic communications and the need to educate young people and staff about the online benefits and risks both within and outside of the College. Online Safety is within the scope of other policies including Keeping Children Safe in Education, Student Behaviour, Child protection, Bullying, Curriculum and Health & Safety.

Please refer to Appendix D for the full Acceptable Use of IT Agreement policy.

Copyright and Licensing

All software and hardware used on the College's system should be correctly licensed. All staff and students should sign an agreement of acceptable use.

1. Principles and Values

The College holds personal data on students, staff and other people to help conduct day-to-day activities. Its loss can result in a data breach by illegal activity to cause harm to individuals, groups or the reputation of the College.

Everybody at St Michael's has a shared responsibility to secure any sensitive information in line with the UK General Data Protection Regulation.

The college has key staff overseeing Online Safety consisting of the Designated Safeguarding Officers (D. Freegard and J. Nottage) and the IT Manager (N. Haxby).

Online Safety depends on effective practice at a number of levels:

- Responsible IT use by all staff and students through education and policies.
- Sound implementation of Online Safety practice in both administration and curriculum.

2. Teaching and learning

2.1 Internet use will enhance and extend learning

Benefits of using the Internet in education include:

- Students' access to remote learning wherever and whenever convenient.
- Impact teachers' pedagogy through classroom practice and professional development for all staff.
- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between students world-wide.
- Access to experts in many fields for students and staff.

- Collaboration across support services and professional associations.
- Exchange of curriculum and administration data with the Local Authority and DfE.

2.2 Students will be taught how to evaluate Internet content

- If staff or students discover unsuitable sites, the URL (address), time, content must be reported to the IT Manager.
- St Michael's Catholic College will strive to ensure that the use of internet derived materials by students and staff complies with copyright law and is free from plagiarism.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and students.

2.3 SEND Students

The College endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the College's Online Safety rules.

However, staff are aware that some students may require differentiated teaching or events where, for example, SEND students have poor social understanding and careful consideration is given to group interactions when raising awareness of Online Safety.

3. Managing Internet Access

3.1 Authorised Internet Access

- The College maintains a current record of all staffs' and students' internet access activity.
- All staff must read and sign the 'Acceptable IT Use Agreement' before using any College IT resources.
- Parents will be informed that students have supervised Internet access and sign paper or electronic consent form for this purpose.
- Students must apply for Internet access individually by agreeing to comply with the responsible Internet use statement when joining the college.
- Staff have the option to use monitoring software to oversee students' desktop activity in line with the behaviour policy. Online Safety matters are referred to the Designated Safeguarding Officers or the IT Manager, if required.

3.2 E-mail

- Students are encouraged to use approved E-mail accounts on the College system.
- Students must immediately tell a teacher if they receive an offensive E-mail.
- Students must not reveal personal details of themselves or others in E-mail communication, or arrange to meet anyone without specific permission.
- Access in college to external personal E-mail accounts may be blocked.
- The sharing of 'viral', social media or mass audience messages with e-mail distribution lists is not permitted.
- E-mail sent to external organisations should be written carefully and in line with professional expectations of teachers and support staff before sending, in the same way as a letter written on college headed paper.

3.3 Social Networking

- The College will filter access to social networking sites (except Google Classroom) unless there is a specific and approved need.
- Students should be advised not to disclose personal details e.g. photos of anyone connected with the College.
- Students should be advised on security, set complex passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Students should be aware of privacy settings and controls for accounts.

3.4 Managing Emerging and Existing Technologies

Emerging or existing technologies will be examined for educational benefit and a UK Data Protection Impact Assessment (DPIA) will be carried out before use in College is allowed:

- Smart devices, games consoles, or other web-enabled devices are discouraged for personal use during lessons or formal College time unless a DPIA is approved. Students are not permitted to use devices on the college premises. Staff are expected to use devices appropriately and in line with professional expectations.
- The sending of abusive or inappropriate electronic communication is forbidden.
- contact@stmichaelscollege.org.uk is the chosen method of electronic communication with parents. EduLink One is also used for this purpose.
- Staff have access to a College phone where contact with students is required.
- Improved access to technical support including remote management of networks and automatic system updates along with appropriate filtering.
- Artificial Intelligence (AI) such as ChatGPT is available for college staff and currently restricted for students on the college network. Students should not use AI to generate responses that can lead to plagiarised work or submitting tasks that have little understanding of learning. The college can use software, such as within Google Classroom, to check for plagiarism.

3.5 Published Content and the College Website

- The contact details on the website will be the College address, e-mail and telephone number. Staff or students' personal information will not be published.
- The Principal and Assistant Principal (Technology for Learning) will take overall editorial responsibility and ensure that the content is accurate and appropriate.

3.6 Publishing Students' Images and Work

- Photographs that include students will be selected carefully and will be appropriate for the context.
- Students' full names will not be used anywhere on the website.
- Written permission from parents or carers will be obtained before photographs of students are published on the College website. This may include the use of online electronic forms via EduLink One.
- Work can only be published with the permission of the student and parents.

3.7 Protecting Personal Data and Preventing Breaches

Personal data will be recorded, processed, transferred and made available according to UK General Data Protection Regulation.

- The College gives relevant staff access to its Management Information System, with a unique ID and password.
- It is the responsibility of staff and students to keep passwords secure. No user ID or accounts should be shared.
- Staff are aware of their responsibility with any form of personal or sensitive data when accessing College data in terms of who has access to it, who it is shared with and the length of time data is stored. This includes any data onsite or offsite pertaining to St Michael's Catholic College.
- A breach of UK GDPR by the Information Commissioner's Office is defined as "likely to result in a high risk of adversely affecting individuals' rights and freedoms".
    - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
- Staff must report any UK GDPR breach that has the potential to cause personal or reputational harm to any individual, group or to St Michael's Catholic College. This must be reported to Mr J. Arda in the first instance, who will then decide whether this needs to be referred to the College's Data Protection Officer.
- The College's Data Protection Officer details are below:
    - Data Protection Officer: SchoolPro
    - Company: SchoolPro TLC Limited

- Address: Unit 1b Aerotech Business Park, Bamfurlong Lane, Cheltenham, GL51 6TU
  Email: DPO@SchoolPro.uk
- Web: www.schoolpro.uk
- Telephone: 01452 947633

A breach or suspected breach of policy by an employee, contractor or student may result in the temporary or permanent withdrawal of college IT hardware, software or services from the offending individual(s).

Any policy breach is grounds for disciplinary action in accordance with the College Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings. The Information Commissioner's Office (ICO) has new powers to issue monetary penalties which came into force on 25 May 2018, allowing it to serve notices requiring organisations to pay up to €20m (£17.5m) or 4% of a company's global turnover for serious breaches of the General Data Protection Regulation.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the UK GDPR;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the UK GDPR;
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern.

3.8 Malicious software

All files downloaded from the Internet, received via e-mail or on removable media (e.g. flash or external hard drive) must be checked for any malicious software using College provided anti-virus or anti-malware software before using them. Users should allow regular updates to occur and contact IT support immediately if any matters arise with college-owned devices. Any individual using lease-to-buy devices should contact the relevant companies for direct support. Home computers must have regular system and updates to protect both users at home and the College from malicious software. Software and security updates must be run frequently on home devices. These checks are the responsibility of individuals using devices at home.

3.9 Remote Access

- All users are responsible for all activity via any remote access facility or EduLink One and ensure access information is both secure and at an appropriate level of security.
- Ensure passwords meet high complexity requirements such as at least eight

characters, a combination of letters, numbers, upper/lower case and special characters.

- Protect College information and data at all times, within and outside of the College, including any printed material produced while using the remote access facility.

3.10 Personal Devices (including smart devices)

- The College allows staff to bring in personal smart devices for their own use. Students are allowed to bring personal smart devices/phones to College but they must be switched off and not used at all during College hours.
- This technology may be used, however, for educational purposes, as mutually agreed with the Principal. For example, sixth form students may use their smart devices in lessons where permitted, by the class teacher, along with prior permission of the bill payer, if applicable.
- The College does not accept responsibility for the loss, damage or theft of any personal smart device.
- Users bringing personal devices into College must ensure there is no inappropriate or illegal content on the device.
- Since September 2021, the College has introduced a one-to-one technology for learning programme. All students are expected to have a laptop. When choosing to use a device, they are subject to the Digital Learning Agreement (Appendix E)

4. Policy Decisions

4.1 Assessing Risks

The College will take all reasonable precautions to prevent access to inappropriate material and cannot guarantee that unsuitable material will never appear on a College computer. The College cannot accept liability for the material accessed, or any consequences of Internet access.

The College will exercise its right to monitor the use of the College's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use is taking place.

4.2 Handling Online Safety Complaints

- Complaints of Internet misuse will be dealt with by the Designated Safeguarding Officers or member of SLT, as appropriate.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with child protection procedures.
- Students and parents will be informed of the complaints procedure.

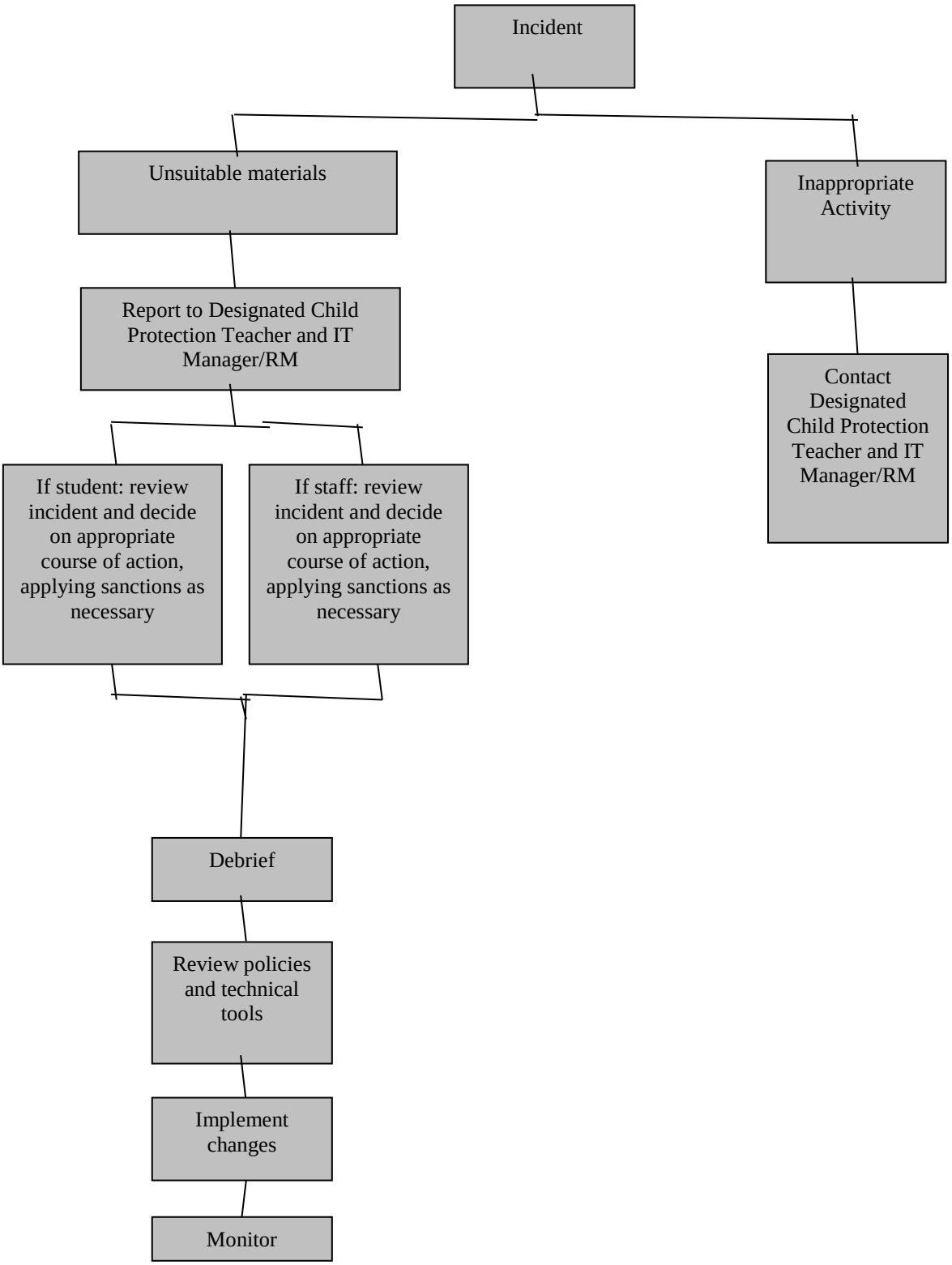
5. Communication of Policy

- The St Michael's Catholic College IT Policy will be available to parents, staff and students on the College website.
- The relevant link is from: https://www.stmichaelscollege.org.uk/gdpr/

Appendices

Referral Process – Appendix A
Online Safety Rules– Appendix B
Letter to parents – Appendix C
Acceptable use of IT Policy for staff, governors and visitors – Appendix D
Digital Learning Agreement – Appendix E

Appendix A
Flowchart for responding to Online Safety incidents in college



Adapted from Becta – E safety 2005

Appendix B

Online Safety Rules

These Online Safety Rules help to protect students and the College by describing acceptable and unacceptable computer use.

- The College sets rules for the use of the network and the Internet.
- It is a disciplinary offence to use a computer or network for a purpose not permitted by the College.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as e-mail could be forwarded to unintended readers.
- Anonymous messages, viral and spam messages are not permitted.
- Users must take care not to reveal personal information through email, social media, instant messaging or over the Internet generally.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes are not permitted.
- Do not share your account details with anybody else or allow anyone to use your account.

Appendix C

St Michael's Catholic College
Student Acceptable Use Agreement

All students use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both students and their parents/carers are asked to sign to show that the Online Safety Rules have been understood and agreed.

Student: ***Tutor Group:***

Students' Agreement

- I have read and I understand the Online Safety Rules and the Digital Learning Agreement.
- I will use the computer, network, smart devices, Internet access, apps and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed: **Date:**

Parent's Consent for Internet Access

I have read and understood the College Online Safety rules available from: https://www.stmichaelscollege.org.uk/gdpr/ and give permission for my son / daughter to access the Internet and use different technologies within the College.

I understand that the College will take all reasonable precautions to ensure that students cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the College cannot be held responsible for the content of materials accessed through the Internet. I agree that the College is not liable for any damages arising from the use of the Internet facilities.

Signed: ***Date:***

Please print name:

Please complete, sign and return to the College

Appendix D

ST MICHAEL'S CATHOLIC COLLEGE
ACCEPTABLE USE OF IT POLICY
FOR STAFF, GOVERNORS AND VISITORS

The Aim
IT and the related technologies such as email, the internet and smart devices are an expected part of our daily working life in the College.

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the College's Online Safety coordinator.

- I will only use the College's email / Internet / Intranet / Learning Platform / app and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal.
- I will comply with the IT system security and not disclose any login details or passwords provided to me by the College or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as a mobile phone number or personal email address to pupils.
- I will not give out my staff pass/lanyard to students.
- I will only use the approved, secure email system(s) for any College business.
- I will ensure that personal or sensitive data (such as data held on SIMS or EduLink One) is kept secure or encrypted in line with the UK General Data Protection Regulation (GDPR) and is used appropriately, whether in the College, emailed, electronically shared or accessed remotely. Personal data can only be taken out of College or accessed remotely when authorised by the Principal or Governing Body.
- I will ensure any personal or sensitive data pertaining to the College is not stored on e.g. USB memory sticks or external hard drives. Any personal or sensitive data that could breach UK GDPR must not be left unattended e.g. incomplete print jobs with technical issues must be reported to IT Support using the email address <it@stmichaelscollege.org.uk> or the IT Manager.
- I will not display or show any personal or sensitive data on a screen or projector to anyone not authorised to view it. This may include students, visitors or other unauthorised personnel.

- I will ensure that I lock the screen of my computer when I am unable to supervise it.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with College policy and the completion of UK Data Protection Impact Assessment (DPIA). Images will not be distributed outside the College network without the permission of the parent/guardian, member of staff or Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Principal or designated person for child protection.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in College and outside College, will not bring my professional role into disrepute.
- I will support and promote the College's Online Safety policy and help pupils to be safe and responsible in their use of IT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of IT throughout the College.

Signature ……..…… Date ……

Full Name ……..... (printed)

Job title…….....

Related policies:

- Freedom of Information Policy
- Data Protection Policy (including UK GDPR)
- Data Breach Policy
- Data Retention Policy
- Social Media Policy
- Online Safety Policy (p. 4-14 in the St Michael's Catholic College IT Policy)
- Acceptable Use of IT Policy for staff, governors and visitors (Appendix D in the St Michael's Catholic College IT Policy)
- Health and Safety Policy

Related documents:

- Privacy Notice for Pupils and Parents
- Privacy Notice for Staff
- Consent form for photos
- Data Breach Report Form

July 2024

Signed: Date:

Chair of the Welfare Committee

Review Date: 2025

Appendix E – Digital Learning Agreement

Updated 22nd June 2023

Rationale

At St Michael's, we want to prepare students for tomorrow's employment opportunities and the future jobs that do not yet exist. The continued pace and growth of technology changes the way we live and work. Therefore, St Michael's is committed to providing every student with use of a Chromebook or their own laptop in the College to cultivate their independence, access study materials at their own pace and approach lesson activities with more flexibility than ever to suit their needs. Creative and innovative ways of learning underpin our teaching and we want students to make the best use of digital learning to support this both within the College and beyond the College day.

To help ensure this programme is successful from our joint support of your son/daughter, we invite you to commit to the principles outlined in this Agreement. As a College we are prepared to provide the facilities and resources needed to make this work, but we also need the commitment of parents and students. This Agreement is between parent/carer, student and the College.

Please note if you/your child provides their own device to use within the college, it is at their own risk. The college is in no way responsible for any damage, loss or theft. Any student causing vandalism/damage to a device within the College premises will be subject to sanctions within the College behaviour policy. Parents/carers will be notified if this Agreement is updated in future.

Students will be reminded by their teachers the lesson before whether to bring a laptop into the next lesson. This will take the form of a Google Classroom notification. As such, students are not expected to bring a laptop unless they have been notified that it will needed in a lesson. Students may bring in their own device, but if they choose not to do so, they will still have access to one in College only. Please follow the link to How to check Google Classroom Announcements

We will provide a chargeable locker for every student for their laptop only. This locker is free for all students. The locker is for the duration of your child's Collegeing at St Michael's. It is a secure place during the College day for devices. **It applies for <u>all</u> students as they are responsible for the key.**

The locker is a charging station, so they can **collect/drop off their laptop only in the morning between 08:30-08:40, during the <u>first half</u> of lunch time, to use in lessons or to take it home/charge it after College**, if they wish. The Chromebook or laptop and the charger will be a student's responsibility. There will be sanctions for loss/damage/inappropriate use, as outlined in the digital learning agreement and the information technology policy.

If eligible for free College meals, a student can be lent a College-owned laptop once a deposit is provided by the parent/carer (parents will be informed

accordingly via EduLink or letter). This deposit is returned by a parent/carer request at the end of the student's Collegeing if the Chromebook has been returned in working order and without damage after the device is checked by the IT Manager or appropriate member of staff. The request is made through an online form which is sent out nearer the time.

If the Chromebook, charger or locker key should be lost or damaged, the parent or carer will need to make a non-refundable payment to replace or repair any damage. A non-refundable payment through ParentPay of £10 is required to replace any lost locker key. The student is also set a Friday and Saturday detention. Costs may vary for the laptop and/or charger, depending on the extent of any damage and any invoice for the required work. The locker is only for storing the laptop and no other items for health and safety reasons.

The 'Chromebook' is a lease-to-buy or College-owned device, which is issued to the pupil as an aid to study both in the College and at home, subject to the following conditions:

The Chromebook may be used *in College and at home* for study purposes, *providing reasonable care is taken to prevent loss or damage.*
"Taking reasonable care" includes:

Ensuring the Chromebook is always transported in an appropriately secure bag.

- Making sure the Chromebook is not subject to careless or malicious damage (e.g. as a result of inappropriate behaviour).
- Reporting any loss or damage (including accidental loss or damage) promptly to the IT Manager.
- Not decorating, customising or allowing any graffiti on the Chromebook or its accessories.
- The student and/or their parent/carer is liable for any repairs needed, if found by the College to be responsible for the damage or misappropriation of the Chromebook. In this event, repairs will not take place until payment is made to the College.
- Persistent and deliberate damage may result in the withdrawal of the Chromebook from the student.
- Taking reasonable precautions to prevent the introduction of computer viruses and, if in any doubt whether a virus or malware has contaminated the Chromebook, reporting the matter to the IT Manager before connecting it again to the College network.
- The device should not be used by anyone other than the named student.

1. Incidents of theft or attempted theft must be reported to a member of the Senior Leadership Team.
2. The IT Manager must be informed immediately of any faults with the Chromebook.
3. The Chromebook must be available for regular health and maintenance checks as arranged by St Michael's Catholic College.
4. Where applicable, any software installed by St Michael's Catholic College should not be removed under any circumstances.
5. The Chromebook must not be used for any illegal and/or anti-social purpose, including access to inappropriate Internet sites. Security software will be installed on the Chromebook which enables St Michael's Catholic College to monitor such activities.
6. Software must not be installed on the Chromebook unless it is your own device with appropriate licences and security software. Software for which you do not have a valid licence is illegal. Checks on the software installed will be made regularly. The College reserves the right to remove any unauthorised software.
7. Students may only participate in this Chromebook scheme whilst they remain at St Michael's Catholic College. If a pupil leaves the College before the end of the Agreement, they are expected to return the Chromebook in good working order unless they have paid for the device

in full under the Freedom Tech arrangement. In the event of significant damage where a student has not been "taking reasonable care" the parent/carer will need to pay for its replacement.

8. The College reserves the right to recall or withdraw the Chromebook at any time, where appropriate. If any changes are made to these terms, the parent or carer will be notified.
9. Students must also follow the St Michael's Catholic College Information Technology Policy. This document is available from https://www.stmichaelscollege.org.uk/statutory-documents/ under Policy Documents.
10. When students are using laptops in lessons (and certainly in the APB) they should expect to have their digital activity closely monitored by staff. Failure to comply with instructions or access in lesson time to sites/activities not directed by their teacher will be sanctioned in line with the College behaviour policy.

If your child is using their own device or 'laptop', it is subject to the following conditions:

The laptop may be used *in College and at home* for study purposes, *providing reasonable care is taken to prevent loss or damage.*

The college does not accept any responsibility for loss or damage to personal technology devices. The responsibility is with the owner of the personal technology or device.

"Taking reasonable care" includes:

- Ensuring the laptop is always transported in an appropriately secure bag.
- Making sure the laptop is not subject to careless or malicious damage (e.g. as a result of inappropriate behaviour or placing items on top of the device).
- Reporting any loss or damage (including accidental loss or damage) promptly to a member of the SLT.
- Not decorating, customising or allowing any graffiti on the laptop or its accessories.
- The student and/or their parent/carer is liable for any repairs needed.
- Persistent and deliberate damage may result in the withdrawal of the laptop from the student.
- Taking reasonable precautions to prevent the introduction of computer viruses and, if in any doubt whether a virus has contaminated the laptop, reporting the matter to the IT Manager before connecting it again to the College network.
- The device should not be used by anyone other than the named student.

1. Incidents of theft or attempted theft must be reported to a member of the Senior Leadership Team. However, the College is in no way responsible for damage, loss or theft.
2. Any faults with the laptop must be managed by the parent/carer.
3. The College will not provide any software to be installed on personal devices.
4. The laptop must not be used for any illegal and/or anti-social purpose, including access to inappropriate Internet sites. It is the parent/carer's responsibility to ensure security updates are carried out regularly and software to monitor threats is run regularly.
5. **Students are expected to bring their laptops to lessons (sufficiently charged) when required by a teacher for a lesson.** The laptop may be connected, charged and stored in one of the College lockers by the student at the end of each day. It may also be left overnight, at owner's risk.
6. If any changes are made to these terms, the parent or carer will be notified.
7. Students must also follow the St Michael's Catholic College Information Technology Policy. This document is available from https://www.stmichaelscollege.org.uk/statutory-documents/ under Policy Documents.

When students are using laptops in lessons (and certainly in the Alternative Provision Base) they should expect to have their digital activity closely monitored by staff. Failure to comply with instructions or access in lesson time to sites/activities not directed by their teacher will be sanctioned in line with the College behaviour policy.

ST MICHAEL'S CATHOLIC COLLEGE
BIOMETRICS POLICY
2023-25

St Michael's Catholic College is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with College's policy review schedule.

A current version of this document is available from:
https://www.stmichaelscollege.org.uk/gdpr/

Signature: Mr J Arda Date: 20/02/2023

Version History Log

Version	Description of Change	Date of Policy Release by Judicium
1	Initial Issue	06.05.18
2	Updated references to UK GDPR	11.05.21
3	Formatting amendments	03.08.22

Biometrics Policy

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns and hand measurements.

All biometric data is considered to be special category data under the UK General Data Protection Regulation (UK GDPR). This means the data is more sensitive and requires additional protection as this type of data could create more significant risks to a person's fundamental rights and freedoms.

This policy complies with The Protection of Freedoms Act 2012 (sections 26 to 28), the Data Protection Act 2018 and the UK GDPR.

The College has carried out a Data Protection Impact Assessment with a view to evaluating whether the use of biometric data is a necessary and proportionate means of achieving the legitimate objectives set out below.

The result of the Data Protection Impact Assessment has informed the college's use of biometrics and the contents of this policy.

What is an Automated Biometric Recognition System?

An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e., electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

The Legal Requirements under UK GDPR

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it.

As biometric data is special category data, in order to lawfully process this data, the College must have a legal basis for processing personal data and a separate condition for processing special category data. When processing biometric data, the College rely on explicit consent (which satisfies the fair processing conditions for personal data and special category data). Consent is obtained using the consent form(s) in the appendix at the end of this document.

The college processes biometric data as an aim to make significant improvements to our canteen and lunch facilities or for pupils to sign in. The reasons are to ensure efficiency and a quicker lunch service, to do away with the need for swipe cards and cash being used, and to safeguard children. In the last case, and at lunch times, the biometric data is used to support vulnerable students to ensure that they consume lunch on a regular basis.

Consent and Withdrawal of Consent

The College will not process biometric information without the relevant consent.

Consent for pupils

When obtaining consent for pupils, both parents will be notified that the College intend to use and process their child's biometric information. The College only require written consent from one parent (in accordance with the Protection of Freedoms Act 2012), provided no parent objects to the processing.

If a parent objects to the processing, then the College will not be permitted to use that child's biometric data and alternatives will be provided.

The child may also object to the processing of their biometric data. If a child objects, the College will not process or continue to process their biometric data, irrespective of whether consent has been provided by the parent(s).

Where there is an objection, the College will provide reasonable alternatives which will allow the child to access the same facilities that they would have had access to had their biometrics been used.

Pupils and parents can also object at a later stage to the use of their child's/their biometric data. Should a parent wish to withdraw their consent, they can do so by writing to the College at contact@stmichaelscollege.org.uk requesting that the College no longer use their child's biometric data.

Pupils who wish for the College to stop using their biometric data do not have to put this in writing but should let Mr Kelly know for the purposes of catering. For any other GDPR related matters, Mr Arda should be contacted.

The consent will last for the time period that your child attends the College (unless it is withdrawn).

Retention of Biometric Data

Biometric data will be stored by the College for as long as consent is provided (and not withdrawn). If/when biometric changes significantly enough as a child grows, a recapture of the data may be required.

Once a pupil leaves, the biometric data will be deleted from the College's system no later than one week.

Storage of Biometric Data

At the point that consent is withdrawn, the College will take steps to delete their biometric data from the system and no later than one week.

Biometric data will be kept securely and systems will be put in place to prevent any unauthorised or unlawful access/use.

The biometric data is only used for the purposes for which it was obtained and such data will not be unlawfully disclosed to third parties.

Appendix 1 – Biometric Consent Form (parent/carer)

Please sign below if you consent to the College taking and using information from your son/daughter's fingerprint as part of an automated biometric recognition system. This biometric information will be used by the College for the purpose of charging for College meals.

In signing this form, you are authorising the College to use your son/daughter's biometric information for this purpose until he/she either leaves the College or ceases to use the system.

If you wish to withdraw your consent at any time, this must be done so in writing and sent to contact@stmichaelscollege.org.uk. Once your son/daughter ceases to use the biometric recognition system, his/her biometric information will be securely deleted by the College no later than one week.

Please note that pupils can object or refuse to allow their biometric data to be taken/used and if they do this, we will provide them with an alternative method of accessing relevant services. This will be discussed with you or your child (depending on their age and their understanding of their data rights) within College. However, we would encourage you to also discuss this with your child at home to ensure that they are aware of their right to refuse or to change their mind at any time.

For further information on the processing of biometric data, please see our Biometrics Policy which is available from: https://www.stmichaelscollege.org.uk/gdpr/

Parental Consent:

Having read the above guidance information, I give consent to information from the fingerprint of my son/daughter being taken and used by the College for use as part of an automated biometric recognition system.

I understand that I can withdraw this consent at any time.

Parent/carer name: …….

Signature: ……..

Date: ……

Name of student: ……

Form group: ……

Please complete a copy of this consent form.

July 2024

Signed: Date:

Chair of the Welfare Committee

Review Date: 2025

ST MICHAEL'S CATHOLIC COLLEGE
COOKIE POLICY 2024-25

Document Owner and Approval

St Michael's Catholic College is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the college's policy review schedule.

A current version of this document is available from:

https://www.stmichaelscollege.org.uk/gdpr/.

Signature: J. Arda Date: 10/07/2023

Version History Log

Version	Description of Change	Date of Policy Release by Judicium
1	Initial issue	06.05.18
2	Addition of one sentence	19.08.21
3	Minor formatting changes	02.08.22

Cookie Policy

We ask that you read this cookie policy carefully as it contains important information on the use of cookies on our website.

What are Cookies?

Cookies are small data files that are placed on your computer or mobile device when you visit a website. Cookies are widely used by online service providers to help build a profile of users. They are also used to make websites work, or work more efficiently, as well as to provide information to the owners of the site. Some of this data will be aggregated or statistical, which means that we will not be able to identify you individually.

You can set your browser not to accept cookies and the information below explains how to remove cookies from your browser. However, some of our website features may not function as a result.

Types of Cookies

The cookies we place on your device fall into the following categories:

- Session cookies — these cookies allow our website to link your actions during a particular browser session. They expire each time you close your browser and do not remain on your device afterwards.
- Persistent cookies — these cookies are stored on your device in between browser sessions. They allow your preferences or actions across our website to be remembered. They will remain on your device until they expire, or until you delete them from your cache.
- Strictly necessary cookies — these cookies are essential for you to be able to navigate our website and use its features. Without these cookies, the services you have asked for could not be provided.
- Performance cookies — these cookies collect information about how you use our website, e.g., which pages you visit most often. These cookies do not collect personally identifiable information about you. All information collected by these cookies is aggregated and anonymous and is only used to improve how our website works.
- Functionality cookies — these cookies allow our website to remember the choices you make (such as your username, language, last action and search preferences) and provide enhanced, more personal features. The information collected by these cookies is anonymous and cannot track your browsing activity on other websites.

The Cookies We Use

The table below provides more information about the cookies we use and why:

The Cookies We Use	What They Do
Google Analytics	This is a web analytics service provided by Google Inc which uses cookies to show us how visitors found and explored our site and how we can enhance their experience. It provides us with information about the behaviour of our visitors (e.g., how long they stayed on the site, the average number of pages viewed) and also tells us how many visitors we have had.
CookieLawInfoConsent	The cookie is set by the GDPR Cookie Consent plugin and is used to store whether or not user has consented to the use of cookies. It does not store any personal data.
cookielawinfo-checkbox-necessary	This cookie is set by GDPR Cookie Consent plugin. The cookies is used to store the user consent for the cookies in the category "Necessary".
viewed_cookie_policy	The cookie is set by the GDPR Cookie Consent plugin and is used to store whether or not user has consented to the use of cookies. It does not store any personal data.

How We Use Your Cookies

The School may request cookies to be set on your computer or device. Cookies are used to let us know when you visit our website, how you interact with us and to make your experience using the school website better for you. The cookies we collect may differ depending on what you are looking at on our website. You are able to adapt your cookie preferences but by blocking certain types of cookies, it may mean that your experience on the website is impacted.

Consent to Use Cookies

We will ask for your permission (consent) to place cookies or other similar technologies on your device, except where they are essential to provide you with a service that you have requested (e.g., to enable you to put items in your shopping basket and to use our check-out process).
There is a notice on our home page which describes how we use cookies and requests your consent to place cookies on your device.

How to Turn Off Cookies

If you do not want to accept cookies, you can change your browser settings so that cookies are not accepted. If you do this, please be aware that you may lose some of the functionality of this website. For further information about cookies and how to disable them please go to the Information Commissioner's webpage on cookies: https://ico.org.uk/for-the-public/online/cookies/. You can disable cookies yourself by following the steps at this link: https://www.aboutcookies.org.uk/managing-cookies.

June 2024

Signed:.. Date

Chair of the Welfare Committee

Review Date: 2025