ST MICHAEL'S CATHOLIC COLLEGE
INFORMATION TECHNOLOGY POLICY 2019-20

1. Aim

As part of the curriculum entitlement, students study computing across the key stages. This comprises of 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

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 good Health and Safety attitudes and practice

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, IT strategy and GDPR
Mr Haxby	ICT Development Manager
Ms Hodsoll	Head of ICT
Ms Ertukhanova	Coordinator of Computer Science

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

Health and Safety

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

E-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. E-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 General Data Protection Regulation 2018.

The college has key staff overseeing E-safety consisting of the Designated Safeguarding Officers (D. Freegard and J. Nottage) and the ICT Development Manager (N. Haxby).

E-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 E-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 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.
- Improved access to technical support including remote management of networks and automatic system updates along with appropriate filtering.
- 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 ICT Development 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 e-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 e-safety.

3. Managing Internet Access

3.1 Authorised Internet Access

- The College will maintain a current record of all staff and students who are granted internet access.
- 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.
- Staff have the option to use RM Tutor as a software to monitor students' desktop activity in line with the behaviour policy. E-safety matters are referred to the Designated Safeguarding Officers or the ICT Development Manager, if required.

3.2 E-mail

- Students may only use approved E-mail accounts on the College system.
- Students must immediately tell a teacher if they receive 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 authorised 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 Data Protection Impact Assessment (DPIA) will be carried out before use in College is allowed:

- Mobile phones, games consoles, or other web-enabled devices will not be used for personal use during lessons or formal College time unless a DPIA is approved.
- 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.

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's or students' personal information will not be published.
- The Principal 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 annually 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 the General Data Protection Regulation 2018.

- 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.
- A breach of 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 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: Craig Stilwell
    - Company: Judicium Consulting Ltd
    - Address: 72 Cannon Street, London, EC4N 6AE
    - Email: dataservices@judicium.com
    - Web: www.judiciumeducation.co.uk
    - Telephone: 0203 326 9174

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 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 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 Viruses

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 viruses using College provided anti-virus software before using them. Users should allow regular virus updates to occur and contact IT support provider immediately if any matters arise. Home computers must have regular system and anti-virus updates to protect both users at home and the College from malicious software.

3.9 Remote Access

- All users are responsible for all activity via the 4Access remote access facility 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 mobile phones)

- The College allows staff to bring in personal mobile phones and devices for their own use. Students are allowed to bring personal mobile 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 my use their mobile devices in lesson where permitted, with prior permission of the bill

payer.
- The College is not responsible for the loss, damage or theft of any personal mobile device.
- Users bringing personal devices into College must ensure there is no inappropriate or illegal content on the device.

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 E-safety Complaints

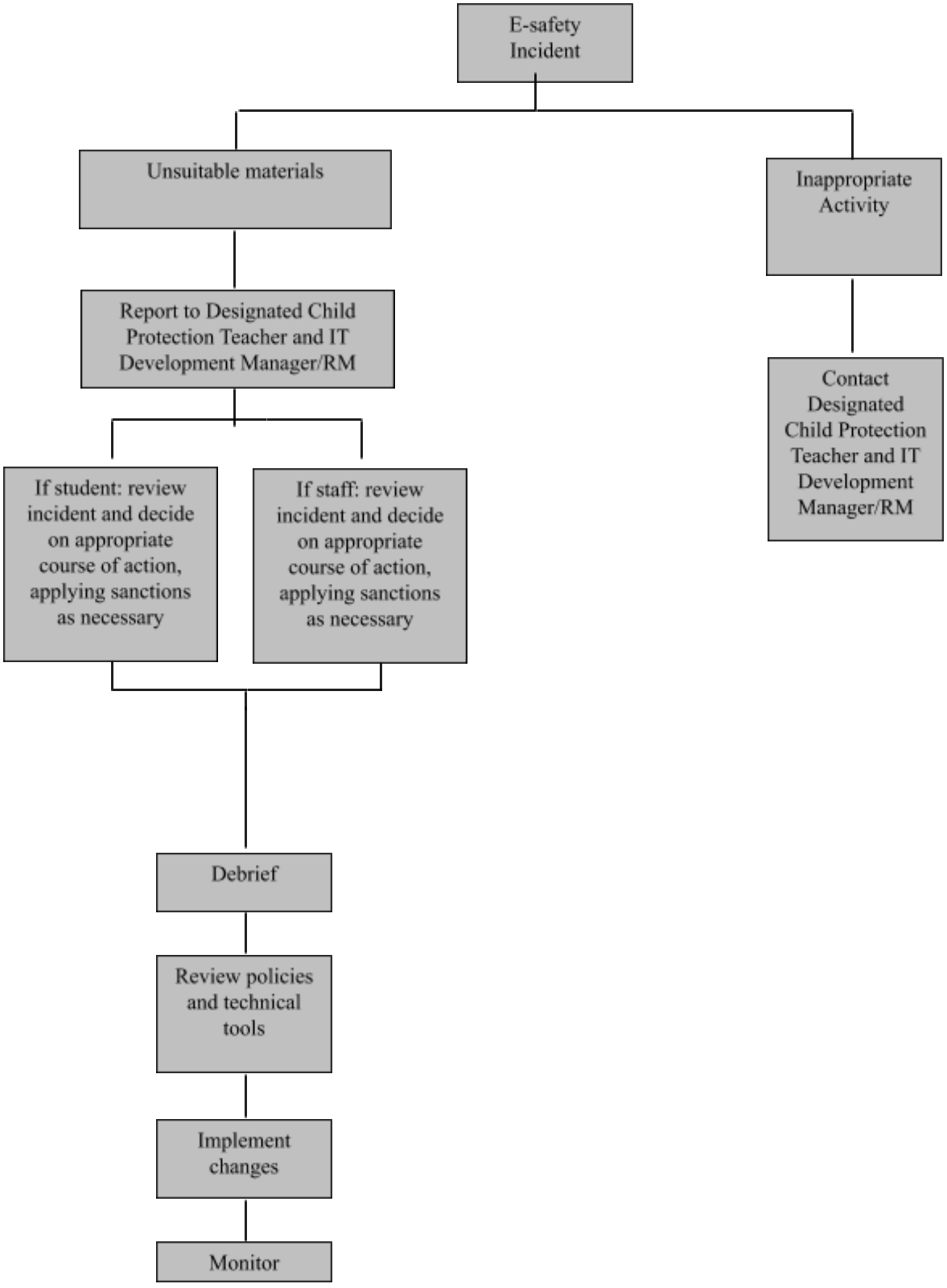
- Complaints of Internet misuse will be dealt with by the Designated Safeguarding Officers or member of the SLT, as appropriate.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with child protection procedures.
- 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
E-safety Rules– Appendix B
Letter to parents – Appendix C
Acceptable use of IT Policy for staff, governors and visitors – Appendix D

Appendix A
Flowchart for responding to E-safety incidents in college



Adapted from Becta – E-safety 2005

Appendix B

E-safety Rules

These E-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 criminal 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 and chain letters 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 is 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 E-safety Rules have been understood and agreed.

Student: ***Tutor Group:***

Students' Agreement

- I have read and I understand the E-safety Rules.
- I will use the computer, network, mobile phones, 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 E-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 mobile 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 e-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 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 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 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 Development 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 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 e-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 (GDPR)
- Data Breach Policy
- Data Retention Policy
- Social Media Policy
- E-Safety Policy (p. 4-14 in the St Michael's Catholic College IT Policy 2018)
- Acceptable Use of IT Policy for staff, governors and visitors (Appendix D in the St Michael's Catholic College IT Policy 2018)
- 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 2019

Date Ratified by the Governors: ……

Signed: ……...

Review Date: September 2020