St Michael's Catholic Primary

With Jesus we can Achieve what we Dream and Believe!

St Michael's Catholic Primary School

ICT Acceptable Use Policy

Contents:

Statement of intent

Here at **St Michael's** we promote the use of technology, as we understand the positive effects it can have on enhancing pupils' learning and community engagement. We have worked so well to embrace technology during lockdown and now have made great strives forward in using it as a foundation for delivering our curriculum. That being said, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly and will be reported to **Nicola Birch** and **Mrs Rigby** in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off St Michael's premises, and applies to all staff, volunteers, contractors and visitors.

Signed by:

Headteacher:_______________ Date: _______________

Chair of governors:_______________ Date: _______________

Review date: _______________

1. Introduction

1.1. This policy applies to all employees, volunteers, supply staff and contractors using St Michael's ICT facilities.

1.2. St Michael's acceptable use policy is divided into the following three sections.

- General policy and code of practice
- Internet policy and code of practice
- Email policy and code of practice

1.3. This policy should be read in conjunction with the St Michael's Data Protection Policy, Privacy Policy and Records Management Policy.

2. General policy and code of practice

2.1. St Michael's has well-developed and advanced ICT systems, which it intends for you to benefit from. These: include:

- Physical devices: Laptops, iPads, Desktop Computers, SLT Mobile Phones.
- Google Apps: Google Chat, Mail, Classroom, Slides, Docs, Sheets, Drive, Calendar and Meet.
- CPOMS, SIMS
- ID card for sign in and navigating both buildings.

2.2. This policy sets out the rules that you must comply with to ensure that the system works effectively for everyone.

Privacy

2.3. The GDPR and Data Protection Act 2018 require all personal and special category data to be processed with the utmost credibility, integrity and accuracy. This applies to all data St Michael's stores on its network regarding staff, pupils and other natural persons it deals with whilst carrying out its functions. All staff at St Michael's should use encrypted data storage units that can be found with **Clare Lafferty** and should be used for storing of "Protected Data". Google Drive can also be used to store this.

2.4. St Michael's will only process data in line with its lawful basis to uphold the rights of both pupils and staff and other third parties.

2.5. In order to protect pupils' safety and wellbeing, and to protect St Michael's from any third party claims or legal action against it, the school may view any data, information or material on St Michael's ICT systems (whether contained in an email, on the network, iPads, mobile phones, notebooks, computers or laptops) and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services. St Michael's Privacy Policy details the lawful basis under which St Michael's is lawfully allowed to do so.

2.6. St Michael's disclaimer that automatically appears at the end of each of your emails notifies the recipient that any email correspondence between you can and may be monitored. You must not remove this disclaimer. You should bring to the attention of any person who wishes or intends to send you an email that **Alyson Rigby or other members of St Michael's SLT** may monitor the content of their email.

Code of practice

St Michael's philosophy	In using ICT, you will follow St Michael's ethos and consider the work and feelings of others. You must not use the system in a way that might cause annoyance or loss of service to other users.
Times of access	The network is available during term time. Out of term time the network will be subject to maintenance downtime and so may not be available for brief periods. If there is availability outside term time **Alyson Rigby, Tom Ferry or MGL** will make staff aware of this.
User ID and password and logging on	You will be given your own St Michael's user ID and password. You must keep these private and not tell or show anyone what they are. This will allow you access to the Network when you are in school and to use printing services, applications and Internet. Your password must be a mix of the following: • Contain at least six characters • A mixture of lower case and capital letters • At least one numbers • At least one symbol If you forget or accidentally disclose your password to anyone else, you must report it immediately to a member of the ICT support staff. You must not use another person's account or allow another person to use your account. The facilities are allocated to you on a personal basis and you are responsible for the use of the machine when you are logged on. St Michael's system records and senior ICT staff monitor your use of the system. Use of St Michael's facilities by a third party using your user name or password will be attributable to you, and you will be held accountable for the misuse. You must not log on to more than one computer at the same time.
User ID and password for logging on when offsite.	**Tom Ferry or MGL** will provide you with a separate "Teacher" account that will have a separate user ID and password that will enable you to log in at home. This will allow you to sign in and use applications and connect to home networks. This is for home use and will not work when return to St Michael's. When using "Protected Data" on home ID, staff should avoid if possible saving any information on hard drive, and instead use Google Drive or external hard drive provided by **Clare Lafferty.**
Printing	Each staff member has a printing pin or code that is linked with their St Michael's user ID. You must select "St Michael's printing server" and then input code/pin into Paperclip application on photocopiers. St Michael's staff should ensure that expensive resources are being used efficiently and the member of staff may suggest other strategies to you to save on resources. Staff should make sure that they do not photocopy in colour from buff paper. White paper can be found in school office with the admin team.

Logging off	You must log off from the computer you are using at the end of each of your sessions and wait for the standard login screen to reappear before leaving. This signals to the system that you are no longer using the service; it ensures security and frees up resources for others to use.
Access to information not normally available	You must not use the system or the internet to find or use facilities or flaws in the system that might give access to information or areas of the network not normally available. You must not attempt to install software to explore or harm the system. Use of hacking tools, e.g. 'loggers', 'sniffers' or 'evidence elimination software', is expressly forbidden.
Connections to the system	You must not connect any hardware which may be detrimental to St Michael's network.
Connections to the computer	You should use the keyboard, mouse and any headphones provided. You must not adjust or alter any settings or switches without first obtaining the written permission of a member of the ICT staff. You must never attempt to use any of the connectors on the back of any desktop computer. You may use USB memory sticks, or other portable storage media where a port is provided on the front of the computers. You are not permitted to connect anything else to the computer without first getting the permission of a member of the ICT staff.
Virus	If you suspect that your computer has a virus, you must report it to a member of the ICT staff immediately.
Installation of software, files or media	You must not install or attempt to install software of any kind to network drives or local hard drives of networked desktop computers. You must not alter or re-configure software on any part of St Michael's system.
File space	You must manage your own file space by deleting old data rigorously and by deleting emails that you no longer require. If you believe that you have a real need for additional space, please discuss this with a senior member of the ICT support staff.
Transferring files	You may transfer files to and from your network home directories using removable devices. When transferring files to and from your network home directories, you must not import or export any material unless the owner of that material expressly permits you to do so.
Reporting faults and malfunctions	You must report any faults or malfunctions in writing to the ICT support staff, including full details and all error messages, as soon as possible.
Food and drink	You must not eat or drink, or bring food or drink, including sweets and chewing gum, into the ICT rooms. You must always maintain a clean and quiet working environment.

Copying and plagiarising	You must not plagiarise or copy any material which does not belong to you.
Copies of important work	It is your responsibility to keep paper copies and back-up copies, e.g. on a CD or memory stick, of your work, and you must keep copies of any important work that you might have. Any data containing personal and special category data must not be stored on unencrypted media and paper back-ups must be stored in a secure lockable location.
Storing Devices	All classrooms at St Michael's have laptop trolleys. These are all lockable and at the end of each day, all child devices and any staff decides that are being left in school overnight/over the weekend/outside term time should be safely locked away.

3. Internet policy and code of practice

3.1. St Michael's can provide access to the internet from desktop PCs, laptops, iPads, Chromebooks and school mobiles via the computer network and through a variety of electronic devices connected wirelessly to the network.

3.2. Staff should not connect personal devices to the school network unless permission has been granted by **Alyson Rigby** and there is no alternative. Whenever accessing the internet using St Michael's or personal equipment you must observe the code of practice below.

3.3. This policy and code of practice is designed to reduce and control the risk of offences being committed, liabilities being incurred, staff or other pupils being offended and St Michael's facilities and information being damaged.

3.4. Any breach of this policy and the code of practice will be treated extremely seriously, and it may result in disciplinary or legal action or expulsion.

3.5. St Michael's may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities St Michael's incurs because of the breach of this policy and code of practice.

Why is internet access available?

3.6. The internet is a large and very useful source of information. Numerous websites and services, both official and unofficial, provide information or links to information which would be useful for educational purposes. It is essential to delivering Home Schooling via Google Meet, Classroom and other Google services.

Why is a code of practice necessary?

There are four main issues:

- Although the internet is often described as 'free', there is a significant cost to St Michael's for using it. This cost includes telephone line charges, subscription costs (which may depend on how much a service is used) and the computer hardware and software needed to support internet access.
- Although there is much useful information on the internet, there is a great deal more material which is misleading or irrelevant. Using the internet effectively requires training and self-discipline. Training is available on request from ICT staff.
- Unfortunately, the internet carries a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle, and to protect to protect the staff and pupils who access to the internet, that it is properly managed. Accessing certain

websites and services, and viewing, copying or changing certain material, could amount to a criminal offence and give rise to legal liabilities. (Smoothwall is our attempt to safeguard against these issues)

- There is a danger of importing viruses on to St Michael's network, or passing viruses to a third party, via material downloaded from or received via the internet, or brought into St Michael's on disks or other storage media.

Code of practice

Use of the internet	The Internet in St Michael's should not normally be used for private or leisure purposes; it is provided primarily for education or business use. You may use the internet for other purposes provided that: • Such use is occasional and reasonable; • Such use does not interfere in any way with your duties; and • You always follow the code of practice. • This can be accessed when in the KS2/1 staff room but staff must not break code of practice.
Inappropriate material	You must not use the internet to access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. "Inappropriate" in this context includes material which is unsuitable for viewing by pupils. You are responsible for rejecting any links to such material which may appear inadvertently during research. If you encounter any material which could be regarded as offensive you must leave that website or service immediately and not make any copy of that material. If you encounter any difficulty in leaving a website or service, you must inform **Tom Ferry or MGL** immediately.
Misuse, abuse and access restrictions	You must not misuse or abuse any website or service or attempt to bypass any access controls or restrictions on any website or service.
Monitoring	The internet access system used by St Michael's maintains a record which identifies who uses the facilities and the use that you make of them. This information is available instantly and is monitored by **Nicola Birth and MGL**. The information collected includes which website and services you visit, how long you remain there and which material you view. This information will be analysed and retained, and it may be used in disciplinary and legal proceedings.
Giving out information	You must not give any information concerning St Michael's, its pupils or parents, or any member of staff when accessing any website or service. This prohibition covers the giving of names of any of these people – the only exception being the use of St Michael's name and your name when accessing a service which St Michael's subscribes to.
Personal safety	You should take care with who you correspond with. You should not disclose where you are or arrange meetings with strangers you have got in contact with over the internet.

Hardware and software	You must not make any changes to any of St Michael's hardware or software. This prohibition also covers changes to any of the browser settings. The settings put in place by St Michael's are an important part of St Michael's security arrangements and making any changes, however innocuous they might seem, could allow hackers and computer viruses to access or damage St Michael's systems.
Copyright	You should assume that all material on the internet is protected by copyright and must be treated appropriately and in accordance with the owner's rights. You must not copy, download or plagiarise material on the internet unless the owner of the website expressly permits you to do so.

4. Email policy and code of practice

4.1. St Michael's computer system enables members of St Michael's to communicate by email with any individual or organisation with email facilities throughout the world.

4.2. For the reason outlined above, it is essential that a written policy and code of practice exists, which sets out the rules and principles for use of email by all.

4.3. Any breach of this policy and code of practice will be treated seriously and it may result in disciplinary or legal action or expulsion.

4.4. St Michael's may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities St Michael's incurs because of the breach of this policy and code of practice.

4.5. Children do not have access to email but do have their own Google Accounts which can be used to access Google Class which has a chat function.

Code of practice

Purpose	You should only use St Michael's email system for work related emails. You are only permitted to send a reasonable number of emails.
Trust's disclaimer	St Michael's email disclaimer is automatically attached to all outgoing emails and you must not cancel or disapply it.
Monitoring	Copies of all incoming and outgoing emails, together with details of their duration and destinations are stored centrally (in electronic form). The frequency and content of incoming and outgoing external emails are checked termly to determine whether the email system is being used in accordance with this policy and code of practice. **Alyson Rigby, SLT** and MGL’s technical staff are entitled to have read-only access to your emails.

Security	As with anything else sent over the internet, emails are not completely secure. There is no proof of receipt, emails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents. As with other methods of written communication, you must make a judgment about the potential damage if the communication is lost or intercepted. Never send bank account information, including passwords, by email.
Program files and non-business documents	You must not introduce program files or non-business documents from external sources on to St Michael's network. This might happen by opening an email attachment or by downloading a file from a website. Although virus detection software is installed, it can never be guaranteed 100 percent successful, so introducing nonessential software is an unacceptable risk for St Michael's. If you need to access additional software, you must contact **Tom Ferry or MGL** in order to get these information. If you have any reason for suspecting that a virus may have entered St Michael's system, you must contact **MGL or Tom Ferry** immediately.
Quality	Emails constitute records of St Michael's and are subject to the same rules, care and checks as other written communications sent by St Michael's. Emails will be checked under the same scrutiny as other written communications. Staff members should consider the following when sending emails: • Whether it is appropriate for material to be sent to third parties • The emails sent and received may have to be disclosed in legal proceedings • The emails sent and received maybe have to be disclosed as part of fulfilling an SAR • Whether any authorisation is required before sending • Printed copies of emails should be retained in the same way as other correspondence, e.g. letter • The confidentiality between sender and recipient • Transmitting the work of other people, without their permission, may infringe copyright laws. • The sending and storing messages or attachments containing statements which could be construed as abusive, libelous, harassment may result in disciplinary or legal action being taken. • Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libelous, malicious, threatening or contravening discrimination legislation or detrimental to the is a disciplinary offence and may also be a legal offence.
Inappropriate emails or attachments	You must not use email to access or send offensive material, chain messages or list-servers or for the purposes of bullying or plagiarising work. You must not send personal or inappropriate information by email about yourself, other members of staff, pupils or other members of St Michael's community. If you receive any inappropriate emails or attachments you must report them to technical staff.
Viruses	If you suspect that an email has a virus attached to it, you must inform the technical staff immediately.
Spam	You must not send spam (sending the same message to multiple email addresses) without the permission of senior staff.

Storage	Old emails may be deleted from St Michael's server after 12 months. You are advised to regularly delete material you no longer require and to archive material that you wish to keep. For further information please see our Records Management Policy.
Message size	Staff are limited to sending messages with attachments which are up to 2Mb in size. If you wish to distribute files within St Michael's, you can do so by using shared areas or by uploading the file to Google Drive. This can then be sent securely.
Confidential Emails	You must ensure that confidential emails are always suitably protected. If working at home or remotely, you should be aware of the potential for an unauthorised third party to be privy to the content of the email. Confidential emails should be deleted when no longer required.
Google Chat	At St Michael's we also have access to Google Chat. The Code of Practice applies to this system as well. All staff must adhere to the Code of Practice when sending chat messages. This are still subject to monitoring in the same way as emails.

5. Email policy – advice to staff

5.1. Staff should remind themselves of the ICT Acceptable Use Policy which relates to the monitoring, security and quality of emails. In addition, staff should be guided by the following good practice:

- Staff should check their emails daily and respond, as appropriate, within a reasonable period if the email is directly addressed to them.
- Staff should avoid spam, as outlined in this policy.
- Staff should avoid using the email system as a message board and thus avoid sending trivial global messages.
- Whilst accepting the convenience of the staff distribution list, staff should try to restrict its use to important or urgent matters.
- Staff should send emails to the minimum number of recipients.
- Staff are advised to create their own distribution lists, as convenient and appropriate.
- Staff should always include a subject line.
- Staff are advised to keep old emails for the minimum time necessary.

6. Further guidelines

- Remember – emails remain a written record and can be forwarded to others or printed for formal use.
- As a rule of thumb, staff should be well advised to only write what they would say face to face and should avoid the temptation to respond to an incident or message by email in an uncharacteristic and potentially aggressive fashion.
- Remember, “tone” can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression.
- Remember that sending emails from your school account is similar to sending a letter on school letterhead, so don't say anything that might bring discredit or embarrassment to yourself or St Michael's.
- Linked with this and given the popularity and simplicity for recording both visual and audio material, staff are advised to remember the possibility of being recorded in all that they say or do.

For further information or to clarify any of the points raised in this policy please speak to the our DPO, Catherine Elison.

Please sign below to confirm you have read and understood St Michael's ICT Acceptable Use Policy:

Signed on behalf of school: ____

Date: ____

Signed by employee/volunteer/contractor/supplier: ____

Print name: ____

Date: ____