ST MICHAEL'S
Church of England High School

ICT and Electronic Devices Policy

"What does the Lord ask of you? To act justly, to love mercy and to walk humbly with your God."
(Micah 6:8)

ST MICHAEL'S
Church of England High School

Contents:

Statement of intent

In our school, our Christian vision shapes all we do. All members of the school community are committed to upholding the St Michael's Church of England Christian values:

- to show love, care and kindness to all in our community
- to value what we have and to share with others
- to enable everyone to achieve their full potential

St Michael's Church of England High School believes that ICT plays an important part in both teaching and learning over a range of subjects, and the school accepts that both school-owned and personally owned electronic devices are widely used by members of staff. The school is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work.

The school has a sensible and practical approach that acknowledges the use of devices, and this policy is intended to ensure that:

- members of staff are responsible users and remain safe while using the internet
- school ICT systems and users are protected from accidental or deliberate misuse, which could put the security of the systems and/or users at risk
- members of staff are protected from potential risks in their everyday use of electronic devices
- a process is in place for claiming financial payments when electronic devices are lost or damaged by members of staff

Personal use of ICT equipment and personal devices is permitted at the school; however, this is strictly regulated and must be done in accordance with this policy, and the Social Media Policy and Online Safety Policy.

Signed by:

	Headteacher	Date: 28/01/2021
	Chair of governors	Date: 28/01/2021

Date of adoption:	28th January 2021
Review date:	January 2024

1. Legal framework

1.1. This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Computer Misuse Act 1990
- The Communications Act 2003
- The Freedom of Information Act 2000
- The Human Rights Act 1998
- Voyeurism (Offences) Act 2019
- DfE (2020) 'Safeguarding and remote education during coronavirus (COVID-19)'
- DfE (2020) 'Keeping children safe in education'
- DfE (2017) 'Special educational needs and disability code of practice: 0 to 25 years'
- DfE (2019) 'School attendance'

1.2. This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Freedom of Information Policy
- Complaints Procedures Policy
- Disciplinary Policy and Procedure
- Online Safety Policy
- Photography and Videos in School Policy
- Securing Breach Prevention and Management Plan
- Records Management Policy

2. Roles and responsibilities

2.1. The governing board has the responsibility for the overall implementation of this policy, ensuring it remains compliant with relevant legislation.

2.2. The headteacher is responsible for:

- reviewing and amending this policy with the Assistant Headteacher, Facilities and Resources (AHFR), Agilisys and DPO, taking into account new legislation, government guidance and previously reported incidents, to improve procedures
- the day-to-day implementation and management of the policy
- the overall allocation and provision of resources. This duty is carried out daily by the AHFR
- handling complaints regarding this policy as outlined in the school's Complaints Procedures Policy
- informing staff that the school reserves the right to access personal devices for the purpose of ensuring the effectiveness of this policy

2.3. The Agilisys is responsible for:

- carrying out daily checks on internet activity of all user accounts and to report any inappropriate use to the headteacher

- monitoring the computer logs on the school's network and to report any logged inappropriate use to the headteacher
- remotely viewing or interacting with any of the computers on the school's network. This may be done randomly to implement this policy and to assist in any difficulties.
- ensuring routine security checks are carried out on all school-owned and personal devices that are used for work purposes to check that appropriate security measures and software have been updated and installed.
- ensuring that, though appropriate steps will be taken to ensure personal information is not seen during security checks, staff are made aware of the potential risks
- accessing files and data to solve problems for a user, with their authorisation
- adjusting access rights and security privileges in the interest of the protection of the school's data, information, network and computers
- disabling user accounts of staff that do not follow the policy, at the request of the headteacher
- assisting the headteacher in all matters requiring reconfiguration of security and access rights and in all matters relating to this policy
- assisting staff with authorised use of the ICT facilities and devices, if required
- immediately reporting any breach of personal data

2.4. The AHFC is responsible for:

- ensuring that all school-owned and personally-owned electronic devices have security software installed, to protect sensitive data in cases of loss or theft
- ensuring that all school-owned devices are secured and encrypted in line with the school's Data Protection Policy
- ensuring that all devices connected to the school network and internet are encrypted.
- ensuring all staff are aware of, and comply with, the data protection principles outlined in the school's Data Protection Policy

2.5. Staff members are responsible for:

- requesting permission from the headteacher or AHFC, subject to their approval, before using school-owned devices for personal reasons during school hours
- requesting permission to loan school equipment and devices from the headteacher or AHFC
- requesting permission from the headteacher, subject to their approval, before using personally-owned devices during school hours and ensuring these devices are submitted for security checks on a termly basis
- ensuring any personally-owned devices that are connected to the school network are encrypted in a manner approved by the data controller
- reporting misuse of ICT facilities or devices, by staff or pupils, to the headteacher
- reading and signing a Device User Agreement to confirm they understand their responsibilities and what is expected of them when they use school-owned and personal devices

2.6. Agilisys is responsible for the maintenance and day-to-day management of the equipment, as well as the loans process.

2.7. The AHFC is responsible for:

- managing a Fixed Asset Register to record and monitor the school's assets. This is maintained by library and Agilisys staff
- overseeing purchase requests for electronic devices
- ensuring value for money is secured when purchasing electronic devices
- monitoring purchases made under the BFS and school financial polices

3. Classifications

3.1. School-owned and personally-owned devices or ICT facilities include, but are not limited to, the following:

- computers/laptops and software
- monitors
- keyboards
- mouses
- scanners
- cameras
- camcorders
- other devices including furnishings and fittings used with them
- mail systems (internal and external)
- internet and intranet (email, web access and video conferencing)
- telephones (fixed and mobile)
- tablets and other portable devices
- fax equipment
- computers
- photocopying, printing and reproduction equipment
- recording/playback equipment
- documents and publications (any type of format)

4. Acceptable use

4.1. The school monitors the use of all ICT facilities and electronic devices. Members of staff will only use school-owned and approved personal devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

- preparing work for lessons, activities, meetings, reviews, etc.
- researching any school-related task
- any school encouraged tuition or educational use
- collating or processing information for school business

4.2. Inappropriate use of school-owned and personal devices could result in a breach of the school's Data Protection Policy.

4.3. Inappropriate use of school-owned and personal devices could result in a breach of legislation, including the UK GDPR and Data Protection Act 2018.

4.4. Any member of staff found to have breached the school's Data Protection Policy or relevant legislation will face disciplinary action.

4.5. This policy applies to any computer or other device connected to the school's network and computers.

4.6. Staff should always be an example of good practice to pupils, serving as a positive role model in the use of ICT and related equipment.

4.7. Since ICT facilities are also used by pupils, the school has acceptable use agreements for pupils and staff will ensure that pupils comply with these.

4.8. Pupils found to have been misusing the ICT facilities will be reported to the headteacher.

4.9. School-owned electronic devices are not used to access any material which is illegal, inappropriate, or may cause harm or distress to others.

4.10. Any illegal, inappropriate or harmful activity is immediately reported to the headteacher.

4.11. Members of staff do not open email attachments from unknown sources.

4.12. Members of staff do not use programmes or software which may allow them to bypass the filtering or security systems.

4.13. Members of staff do not upload or download large capacity files (over 500MB) without permission from Agilisys.

4.14. All data is stored appropriately in accordance with the school's Data Protection Policy.

4.15. Members of staff only use school-owned electronic devices to take pictures or videos of people who have given their consent.

4.16. School-owned electronic devices are not used to access personal social media accounts.

4.17. Personal electronic devices are not used to communicate with pupils or parents, including via social media.

4.18. Staff representing the school online will express neutral opinions and will not disclose any confidential information or comments regarding the school, or any information that may affect its reputability.

4.19. Staff will ensure the necessary privacy settings are applied to any social networking sites.

4.20. Images or videos of pupils, staff or parents will only be published online for the activities which consent has been sought.

4.21. Staff will not give their home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be done through authorised school contact channels.

4.22. Copyrighted material is not downloaded or distributed.

4.23. School-owned devices can be taken home for work purposes only, once approval has been sought from the headteacher and Agilisys. Remote access to the school network will be given to staff using these devices at home.

4.24. School equipment that is used outside the premises, e.g. laptops, will be returned to the school when the employee leaves employment, or if requested to do so by the headteacher.

4.25. While there is scope for staff to utilise school equipment for personal reasons, this will not be done during working hours unless approved by the headteacher or in the case of a personal emergency.

4.26. Private business must not be mixed with official duties, e.g. work email addresses should be reserved strictly for work-based contacts only.

4.27. Personal use of school-owned equipment can be denied by the headteacher at any time. This will typically be because of improper use or over-use of school facilities for personal reasons. A charge may be made for using equipment if the values are significant.

4.28. Where permission has been given to use the school equipment for personal reasons, this use should take place during the employee's own time, e.g. during lunchtime or after school. Where this is not possible, or in the case of an emergency, equipment can be used for personal reasons during work hours provided that disruption to the staff member's work, and the work of others, is minimal.

4.29. Abuse of ICT facilities or devices could result in privileges being removed. Staff should be aware of acceptable ICT use, and misuse of the facilities, as defined in this policy, must be reported to the headteacher.

4.30. More details about acceptable use can be found in the staff Technology Acceptable Use Agreement and Device User Agreement.

4.31. Failure to adhere to the rules described in this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

5. Emails and the internet

5.1. The school email system and internet connection are available for communication and use on matters directly concerned with school business.

5.2. Emails will not be used as a substitute for face-to-face communication, unless it is otherwise impossible.

5.3. Hasty messages will not be tolerated. All emails will be written in a professional tone and will be proof read by the staff member sending the email to ensure this prior to sending.

5.4. Abusive messages will not be tolerated – any instant of abuse may result in disciplinary action.

5.5. If any email contains confidential information, the user must ensure that the necessary steps are taken to protect confidentiality.

5.6. The school will be liable for any defamatory information circulated either within the school or to external contacts.

5.7. The school email system and accounts must never be registered or subscribed to spam or other non-work-related updates, advertisements or other personal communications. School email

addresses must not be shared without confirming that they will not be subjected to SPAM or sold on to marketing companies.

5.8. All emails that are sent or received will be retained within the school for a period of six months dependent on the information contained. More information can be found in the Records Management Policy. The timeframe will be altered where an inbox becomes full.

5.9. Personal email accounts will only be accessed via school computers outside of work hours and only if they have built-in anti-virus protection approved by the ICT technician. Access to personal emails must never interfere with work duties.

5.10. Staff linking work email accounts to personal devices, subject to the headteacher's approval, will sign the Device User Agreement and submit their devices for routine security checks on a termly basis.

5.11. The types of information sent through emails to a personal device will be limited to ensure the protection of personal data, e.g. pupils' details.

5.12. Contracts sent via email or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between the sender, or the school, and the recipient. Staff must never commit the school to any obligations by email or the internet without ensuring that they have the authority to do so.

5.13. Purchases for school equipment are only permitted to be made online with the permission of the headteacher, and a receipt must be obtained, in order to comply with monitoring and accountability. Hard copies of the purchase must be made, for the purchaser and the AHFR. This is in addition to any purchasing arrangement followed according to the BSF and school financial policies.

5.14. Any suspicious emails will be recorded in the incident log and will be reported to the headteacher. All incidents will be responded to in accordance with the Online Safety Policy.

6. Portable equipment

6.1. All data on school-owned equipment is synchronised with the school server and backed up once a month.

6.2. Portable school-owned electronic devices are not left unattended, are kept out of sight, and are securely locked in a classroom when they are not in use.

6.3. Portable equipment is transported in its protective case, if supplied.

6.4. Where the school provides mobile technologies, such as phones, laptops and personal digital assistants, for off-site visits and trips, only these devices are used.

7. Personal devices

7.1. Staff members will use personal devices in line with the school's **Security Breach Prevention and Management Plan**.

7.2. All personal devices that are used to access the school's online portal, systems, or email accounts, i.e. laptops, will be declared and approved by the headteacher before use and submitted for the routine checks outlined in section 16 of this policy.

7.3. Staff using their own devices will sign an agreement stating that they understand the requirement for routine security checks to take place and the possibility of their personal information being seen by Agilisys. They will be required to provide consent to their device being accessed – if consent is refused, they will not be permitted to use a personal device.

7.4. Approved devices must be secured with a password or biometric access control, e.g. fingerprint scanner.

7.5. Members of staff will not contact pupils or parents using their personal devices.

7.6. Personal devices are only used for off-site educational purposes when mutually agreed with the headteacher.

7.7. Inappropriate messages are not sent to any member of the school community.

7.8. Permission is sought from the owner of a device before any image or sound recordings are made on their personal device. Consent is also obtained from staff, pupils and other visitors if photographs or recordings are to be taken.

8. Removable media

8.1. Removable media is not used in school to ensure a high level of data control.

9. Cloud-based storage

9.1. The school is aware that data held in remote and cloud-based storage is still required to be protected in line with the UK GDPR and DPA 2018.

9.2. Members of staff ensure that cloud-based data is kept confidential and no data is copied, removed or adapted.

10. Remote access

10.1. St Michael's Church of England High School does not make provision for all its systems and services to be made available remotely to all users with remote access permission.

10.2. With regard to availability and speed of remote access services, it should be borne in mind that these may be reliant on 3rd party factors such as the users Internet Service Provider connectivity and/or domestic networking hardware such as routers/switches.

Available Remote Services

10.3. The privilege of remote access is at the discretion of the Head Teacher and access is dependent on their current network and system permissions and access rights.

10.4. Senior Leadership Team has access to the following:-

- Go 4 Schools staff area
- Google drive SLT shared area
- Google drive staff shared area
- Google Classroom
- Microsoft Teams

10.5. Support staff have access to the following:-

- Go 4 Schools staff area
- Google drive staff shared area
- Google classroom

External Users (Local Authority)

10.6. The default situation for external users (typically the SIPS team) is that they are given no ad-hoc remote access to St Michael's systems. If remote access is required, agreed dates and times will be set and the relevant user account will be enabled (in Active Directory) and promptly disabled once the work is complete.

Methods of Remote Access

10.7. Remote access to the St Michael's Church of England High School network is provided by encrypted, secure web based portals.

10.8. Remote access users must sign in via the gateway using a valid St Michael's Active Directory username and password.

Remote Access for 3rd Party and Systems Suppliers

10.9. If possible, recently purchased software that requires external connectivity via a secured line should be provided onsite, as opposed to being performed using remote access. If this is not possible, remote access that allows installations should be monitored until the completion of the installation and the remote session has ended.

10.10. Existing systems suppliers remotely accessing St Michael's systems services must contact the school and inform of the changes that are to be made along with times and dates of the required remote access session.

10.11. User accounts for system suppliers and support should be kept disabled when not in use.

User responsibilities and good working practices

10.12. Staff will follow the guidelines in section 4 of this policy when accessing the school network remotely.

Removal of remote access rights

10.13. Access rights to for remote access may be changed or removed by St Michael's from any authorised/unauthorised user at any time if a breach of the conditions of use has been performed or that user's access is compromising the confidentiality, integrity and/or availability of the St Michael's systems or services.

10.14. The remote access rights of all employees and third party users shall be removed upon termination of employment, contract, or agreement.

11. Live online lessons

11.1. **Systems and technology**

11.1.1. Staff will be told to only download software for live online lessons from a trusted source, e.g. Apple App Store, Google Play or the provider's official website.

11.1.2. The AHFR and Deputy Headteacher, Teaching and Learning will research the best provider to use for live online lessons, taking into account ease of use, privacy measures and suitability for the purposes of live online lessons.

11.1.3. Staff will ensure privacy settings are adjusted appropriately on the provider's site or application.

11.1.4. Staff will ensure their live online lesson service account is protected with a strong password, and will not autosave their password on any device.

11.1.5. Staff will ensure they test and understand the service before conducting their first live online lesson using the 'test' function, where applicable.

11.1.6. Staff will ensure they understand how to mute the microphone and turn off their camera on their device before their first live online lesson.

11.1.7. The AHFR and Deputy Headteacher, Teaching and Learning will teach staff what features are available to them through the school's chosen live online lesson system, e.g. recording calls, sharing files or screensharing.

11.1.8. The school will ensure all pupils due to attend live online lessons have access to equipment that will enable them to participate, e.g. a laptop and internet access, to ensure they do not fall behind their peers who do have access.

11.1.9. Staff will ensure streaming and online chat functions are disabled for pupils.

11.2. **Safeguarding**

11.2.1. Staff will always have due regard for the school's Child Protection and Safeguarding Policy whilst conducting live online lessons.

11.2.2. The planning of live lessons will always be carried out in conjunction with the school's DSL.

11.2.3. The school will ensure the system used for live online lessons does not have a minimum age requirement above the age bracket of pupils attending the lesson.

11.2.4. Pupils will be reminded not to share private information through the live online lesson system by the teacher.

11.2.5. The teacher will remind pupils will not to respond to contact requests from people they do not know when using systems for live online lessons.

11.2.6. Pupils will be informed of the reporting lines, should they see or hear anything inappropriate during live online lessons, via email. Pupils will be provided with the email address of the DSL to report any concerns.

11.2.7. Staff will ensure all video and phone calls are not set to public, and meetings are protected with passwords. Meeting links and passwords will not be published publicly.

11.2.8. Support staff will be on hand to supervise and handle any sudden changes or developments, such disputes between pupils, that may occur during the live online lesson.

11.2.9. Staff will be reminded of their safeguarding obligations and they will report any incidents or potential concerns to the DSL in line with the school's Child Protection and Safeguarding Policy.

11.3. **Personal data**

11.3.1. Staff will have due regard for the school's Data Protection Policy at all times whilst conducting live online lessons.

11.3.2. The school will obtain consent from parents to conduct any live online lessons via email or letter.

11.3.3. The school will communicate the details of how to access the live online lesson and any additional information regarding online learning to parents and pupils via email.

11.3.4. The school will obtain consent from parents if any images or identifying information about any pupil may be used during the live online lesson, e.g. by using video conferencing, via email or letter.

11.3.5. The school will provide pupils with a school email address and login for the chosen live online lesson platform to ensure no personal email addresses or usernames are used by pupils.

11.3.6. Staff will ensure data is only transferred between devices if it is necessary to do so for the purposes of live online lessons, e.g. to report anything serious that has taken place during the online lesson.

11.3.7. Any data transferred between devices will be suitably encrypted. Where this is not possible, other data protection measures will be in place, such as using initials of pupils instead of full names.

11.3.8. When recording a live lesson is necessary, prior permission will be acquired from parents in writing via email and all members of the live lesson will be notified before the lesson commences via email, and again once they have joined the live online lesson.

11.4. **Pupil conduct**

11.4.1. The school will provide pupils with a copy of the Pupil Code of Conduct via email to ensure they understand their responsibilities with regards to conduct during live online lessons.

11.4.2. The school will ensure that pupils sign and return the Technology Acceptable Use Agreement – Pupils prior to taking part in live online lessons.

11.4.3. Pupils will be reminded that they should not be taking part in live online lessons if they are in an inappropriate setting, e.g. a bedroom.

11.4.4. Pupils will be reminded not to record live online lessons on their devices.

11.4.5. Pupils will be reminded not to speak during live online lessons unless they are prompted to do so or have a question about the lesson.

11.4.6. Pupils will be reminded to adhere to the school's Behaviour Management Policy at all times during live online lessons, as they would during a normal school day.

11.4.7. The school will ensure that any pupils who breach the code of conduct will be disciplined in line with the school's Behaviour Management Policy.

11.5. **Staff conduct**

11.5.1. Staff will be required to re-read the Staff Code of Conduct policy and guidance prior to carrying out live online lessons to ensure they understand their responsibilities with regards to conduct during live online lessons.

11.5.2. The school will ensure that staff read, sign and return the Technology Acceptable Use Agreement – Staff prior to commencing live online lessons.

11.5.3. Staff will only use school-provided email addresses and phone numbers to communicate with pupils when conducting live online lessons.

11.5.4. Staff will only use school-owned devices for conducting live online lessons, where possible.

11.5.5. Staff will not share personal information whilst conducting live online lessons.

11.5.6. Staff will conduct live online lessons with appropriate surroundings, e.g. sitting somewhere with a neutral background.

11.5.7. Staff will communicate with pupils within school hours as far as possible (or within hours agreed with the school to suit the needs of staff).

11.5.8. Staff will only communicate and conduct live online lessons through channels approved by the SLT.

11.5.9. Staff will not commence online lessons until at least one other member of staff is in the live lesson 'room', and never without confirmation that at least one other colleague is aware that the live online lesson is taking place.

11.5.10. Staff will keep a log of everything that happens during live online lessons and ensure it is properly documented in line with the school's Records Management Policy.

11.6. **Pupils with SEND**

11.6.1. The school will ensure pupils with SEND receive any additional support with live online lessons where needed, e.g. from an additional member of staff within the live online lesson via phone call.

11.6.2. Staff will be sensitive to the needs of any pupils who may be sensitive to certain topics or issues that may arise during live online lessons.

11.6.3. The SLT, teacher, and SENCO will consider whether one-to-one lessons are appropriate in some circumstances for pupils with SEND.

11.6.4. Additional measures will be considered for pupils with SEND to mitigate the risk of pupils falling behind their peers in terms of education, e.g. text transcripts being used in video lessons.

12. Return of assets to St Michael's Church of England High School

12.1. All St Michael's owned systems and other devices and information/data must be returned to St Michael's upon termination of employment or contract.

12.2. St Michael's systems should be returned prior to the user leaving for critical system updates or re-imaging.

12.3. Before returning the system, users should remove their own personal data from the system.

13. Storing messages

13.1. Emails and messages stored on school-owned devices will be stored digitally or in a suitable hard copy file and disposed of after no more than six months.

13.2. Information and data on the school's network and computers will be kept in an organised manner and should be placed in a location of an appropriate security level.

13.3. If a member of staff is unsure about the correct message storage procedure, help will be sought from Agilisys.

13.4. Employees who feel that they have cause for complaint as a result of any communications on school-owned devices will raise the matter initially with the headteacher, as appropriate. The complaint will then be raised through the grievance procedure.

14. Unauthorised use

14.1. Staff are not permitted, under any circumstances, to:

- use the ICT facilities for commercial or financial gain without the explicit written authorisation from the headteacher
- physically damage ICT and communication facilities or school-owned devices
- relocate, take off-site, or otherwise interfere with the ICT facilities without the authorisation of Agilisys or headteacher. Certain items are asset registered and security marked; their location is recorded by the AHFR for accountability. Once items are moved after authorisation, staff have a responsibility to notify the AHFR of the new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.
- use or attempt to use someone else's user account. All users of the ICT facilities will be issued with a unique user account and password. The password must be changed at regular intervals. User account passwords must never be disclosed to or by anyone.

- use the ICT facilities at any time to access, download, send, receive, view or display any of the following:
    - any material that is illegal
    - any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
    - online gambling
    - remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
    - any sexually explicit content, or adult or chat-line phone numbers
- generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else
- install hardware or software without the consent of Agilisys or the headteacher
- introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the school's computers
- use or attempt to use the school's ICT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.
- purchase any ICT facilities without the consent of the AHFR or headteacher. This is in addition to any purchasing arrangements followed according to the BSF and school financial policies.
- use or attempt to use the school's phone lines for internet or email access unless given authorisation by the headteacher. This includes using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.
- use any chat-lines, bulletin boards or pay-to-view sites on the internet. In addition, staff must not download or attempt to download any software.
- use the internet for any auctioning activity or to purchase items unless given authority to do so by the headteacher. This is in addition to any purchasing arrangement followed according to the BSF and school financial policies.
- knowingly distribute or introduce a virus or harmful code onto the school's network or computers. Doing so may result in disciplinary action, including summary dismissal.
- use the ICT facilities for personal use without the authorisation of the headteacher. This authorisation must be requested on each occasion of personal use.
- copy, download or distribute any material from the internet or email that may be illegal to do so. This can include computer software, music, text, and video clips. If it is not clear that you have permission to do so, or if the permission cannot be obtained, do not do so.
- use, or attempt to use, the communication facilities to call overseas without the authorisation of the headteacher.

- to obtain and post on the internet, or send via e-mail, any confidential information about other employees, the school, its customers or suppliers
- interfere with someone else's use of the ICT facilities
- be wasteful of ICT resources, particularly printer ink, toner and paper
- use the ICT facilities when it will interfere with your responsibilities to supervise pupils
- share any information or data pertaining to other staff or pupils at the school with unauthorised parties. Data will only be shared for relevant processing purposes
- operate equipment to record an image beneath a person's clothing with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks without their knowledge or consent (whether exposed or covered by underwear) – otherwise known as "upskirting"

14.2. Any unauthorised use of email or the internet is likely to result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy and Procedure.

14.3. If a member of staff is subjected to, or knows about harassment, upskirting or bullying that has occurred via staff email or through the use of school-owned devices, they are encouraged to report this immediately to the headteacher.

15. Safety and security

15.1. The school's network will be secured using firewalls in line with the Security Breach Prevention and Management Plan.

15.2. Filtering of websites, as detailed in the Security Breach Prevention and Management Plan, will ensure that access to websites with known malware are blocked immediately and reported to Agilisys.

15.3. Approved anti-virus software and malware protection must be used on all approved devices and will be updated on a termly basis.

15.4. The school will use mail security technology to detect and block any malware transmitted via email – this will be reviewed on a termly basis.

15.5. Members of staff must ensure that all school-owned electronic devices are made available for anti-virus updates, malware protection updates and software installations, patches or upgrades, on a termly basis.

15.6. Approved personal devices will also be submitted on a termly basis, to Agilisys, so that appropriate security and software updates can be installed to prevent any loss of data. Consent for such access will be obtained before the approval of a device – if consent if refused, the school reserves the right to decline a request to use a personal device.

15.7. Records will be kept detailing the date and time, owner of a device and device type, on which the routine checks have taken place – these will be stored in the ICT office.

15.8. Programmes and software are not installed on school-owned electronic devices without permission from Agilisys.

15.9. Staff are not permitted to remove any software from a school-owned electronic device without permission from Agilisys.

15.10. Members of staff who install or remove software from a school-owned electronic device without seeking authorisation from Agilisys, may be subject to disciplinary measures.

15.11. All devices must be secured by a password or biometric access control.

15.12. Passwords must be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.

15.13. Devices must be configured so that they are automatically locked after being left idle for a set time of no more than five minutes for mobile or other portable devices and 10 minutes for desktop computers or laptops.

15.14. All devices must be encrypted using a method approved by the AHFR.

15.15. Further security arrangements are outlined in the Security Breach Prevention and Management Plan.

16. Loss, theft and damage

16.1. For the purpose of this policy, 'damage' is defined as any fault in a school-owned electronic device caused by the following:

- connections with other devices, e.g. connecting to printers which are not approved by Agilisys
- unreasonable use of force
- abuse
- neglect
- alterations
- improper installation

16.2. The school's insurance covers school-owned electronic devices that are damaged or lost, during school hours, if they are being used on the school premises. All claims will include a £300 excess charge.

16.3. Staff members must use school-owned electronic devices within the parameters of the school's insurance cover - if a school-owned electronic device is damaged or lost outside of school hours or off-site, the member of staff at fault may be responsible for paying damages.

16.4. Any incident which leads to a school-owned electronic device being lost is treated in the same way as damage.

16.5. The AHFR and headteacher will decide whether a device has been damaged due to the actions described above.

16.6. Agilisys is contacted if a school-owned electronic device has a technical fault.

16.7. If it is decided that a member of staff is liable for the damage, they are required to pay 20 percent of the total repair or replacement cost.

16.8. A written request for payment is submitted to the member of staff who is liable to pay for damages.

16.9. If the member of staff believes that the request is unfair, they can make an appeal to the headteacher, who makes a final decision within two weeks.

16.10. In cases where the headteacher decides that it is fair to seek payment for damages, the member of staff is required to make the payment within six weeks of receiving the request.

16.11. Payments are made to the AHFR via the finance office, and a receipt is given to the member of staff.

16.12. The school accepts payments made via cheques, cash, and ParentPay.

16.13. A record of the payment is made and stored in the finance office for future reference.

16.14. The headteacher may accept the payment in instalments.

16.15. The member of staff may not be not permitted to access school-owned electronic devices until the payment has been made.

16.16. In cases where a member of staff repeatedly damages school-owned electronic devices, the headteacher may decide to permanently exclude the member of staff from accessing devices.

16.17. If a school-owned device is lost or stolen, or is suspected of having been lost or stolen, the DPO must be informed as soon as possible to ensure the appropriate steps are taken to delete data from the device that relates to the school, its staff and its pupils, and that the loss is reported to the relevant agencies.

16.18. The school is not responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, removable media, etc.

17. Implementation

17.1. Staff are requested to report any breach of this policy to the headteacher.

17.2. Regular monitoring and recording of email messages will be carried out on a random basis. Hard copies of email messages can be used as evidence in disciplinary proceedings.

17.3. Use of the telephone system is logged and monitored.

17.4. Use of the school internet connection is recorded and monitored.

17.5. The AHFR will conduct random checks of asset registered and security marked items.

17.6. Agilisys checks computer logs on the school network on a termly basis.

17.7. Unsuccessful and successful log-ons are logged on every computer connected to the school's network.

17.8. Unsuccessful and successful software installations, security changes and items sent to the printer are also logged.

17.9. Agilisys can remotely view or interact with any of the computers on the school's network. This may be used randomly to implement this policy and to assist in any difficulties.

17.10. The school's network has anti-virus software installed with a centralised administration package; any virus found is logged to this package.

17.11. The school's database systems are computerised. Unless given permission by the AHFR, members of staff must not access the system. Failure to adhere to this requirement may result in disciplinary action.

17.12. All users of the database system will be issued with a unique individual password, which must be changed at regular intervals. Staff must not, under any circumstances, disclose this password to any other person.

17.13. Attempting to access the database using another employee's user account/password without prior authorisation is likely to result in disciplinary action, including summary dismissal.

17.14. User accounts are accessible by the headteacher and Agilisys.

17.15. Users must ensure that critical information is not stored solely within the school's computer system. Hard copies must be kept or stored separately on the system. If necessary, documents must be password protected.

17.16. Users are required to be familiar with the requirements of the UK GDPR and Data Protection Act 2018, and to ensure that they operate in accordance with the requirements of the regulations and the Data Protection Policy.

17.17. Any breach of the rules in this policy may result in disciplinary action, which may lead to dismissal.

17.18. A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the school.

18. Monitoring and review

18.1. This policy is reviewed every three years by the AHFR, Agilisys and the headteacher.

18.2. Any changes or amendments to this policy will be communicated to all staff members by the headteacher.

18.3. The scheduled review date for this policy is January 2024.

Appendix 1: Staff Declaration Form

All members of staff are required to sign this form before they are permitted to use electronic devices that are owned by the school.

By signing this form, you are declaring that you have read, understood and agree to the terms of the ICT and Electronic Devices Policy. You should read and sign the declaration below before returning it to the school office.

Members of staff are required to re-sign this declaration form if changes are made to the policy.

I have read name of school's ICT and Electronic Devices Policy and understand that:

- school equipment must not be used for the fulfilment of another job or for personal use, unless specifically authorised by the headteacher
- illegal, inappropriate, or unacceptable use of school or personal equipment will result in disciplinary action
- the school reserves the right to monitor my work emails, phone calls, internet activity, and document production
- passwords must not be shared and access to the school's computer systems must be kept confidential
- I must act in accordance with this policy at all times

Name of staff:	
Job title:	
Department:	
Signed:	
Agilisys signed:	
Headteacher signed:	
Date signed:	

Appendix 2: Device User Agreement – Staff

This agreement is between St Michael's Church of England High School and **name of staff member** and is valid for the academic year of **2020/2021**.

The school has created this agreement to ensure that **name of staff member** understands their responsibilities when using both school-owned and personal devices, such as mobile phones and tablets, for work purposes whether on or off the school premises.
Please read this document carefully, ensuring you understand what is expected, and sign below to show you agree to the terms outlined.

The school
The school retains sole right of possession of any school-owned device and may transfer the device to another teacher if you do not, or are unable to, for any reason, fulfil the requirements of this agreement.

Approval from the headteacher must be sought before the use of a personal device can commence. The school reserves the right to access personal devices for the purpose of conducting routine security checks, so that appropriate security and software updates can be installed to prevent any loss of data.

Under this agreement, the school will:

- provide devices for your sole use while you are a permanent full-time or part-time teacher at the school
- ensure devices are set up to enable you to connect to, and make effective use of, the school network – remote access to the network will be given to staff using school-owned devices at home
- ensure the relevant persons, such as Agilisys, have installed the necessary security measures on any school-owned or personal device before your use – including, but not limited to, the following:
    - firewalls
    - malware protection
    - user privileges
    - filtering systems
    - password protection and encryption
    - mail security technology
    - tracking technology
- ensure that all devices undergo the following regular checks and updates by Agilisys in line with school policy:
    - termly updates to malware protection
    - termly software updates
    - annual password re-set requirements
    - termly checks to detect any unchanged default passwords
    - malware scans in line with specific requirements
- plan and manage the integration of devices into the school environment, and provide the professional development required to enable you to use the devices safely and effectively

- when required, expect you to pay an excess for accidental damage or loss repair/replacement costs, where loss or damage of a school-owned device is a result of your own negligence
- ensure that any personal device you access the school network from is appropriate and submitted on a termly basis to Agilisys so that appropriate security checks can take place

Under this agreement, you will:

Overall use and care of school-owned devices

- Bring the device and charging unit to the school each day and keep the device with you, or within your sight, at all times.
- Transport the device safely using the cover and carry case, if necessary, issued with the device.
- Not permit any other individual to use the device without your supervision, unless agreed by the headteacher.
- Take responsibility for any other individual using the device.
- Provide suitable care for the device at all times and not do anything that would permanently alter it in any way.
- Lock the device screen when not in use with a passcode.
- Keep the device clean.
- Ensure all devices are switched off or set to silent mode during school hours.
- Immediately report any damage or loss of the device to the AHFR.
- Ensure any tracking technology applied is active at all times.
- Immediately report any viruses or reduced functionality following a download or access to a site, to Agilisys.
- Be prepared to cover the insurance excess, repair or replacement of the device when the damage or loss has been a result of your own negligence.
- Make arrangements for the return of the device and passcode to the AHFR if your employment ends.

Using school-owned and personal devices

- Only use the devices that have been permitted/approved for your use by the headteacher.
- Only use devices for educational purposes.
- Only use apps that are compliant with data protection legislation and from reputable sources.
- Ensure that any personal data is stored in line with data protection legislation.
- Only store sensitive personal data on your device where absolutely necessary and which is encrypted.
- Ensure any school data stored on a device is encrypted and pseudonymised.
- Give permission for Agilisys to erase and wipe data off your device if it is lost, or as part of exit procedures.
- Allow Agilisys to access your personal device (if applicable), to conduct routine security checks to prevent data loss.
- Provide consent and confirm you understand that, if you are using a personal device for work purposes, Agilisys requires access to your device to conduct routine security checks and that there is a potential for your personal information to be seen.
- Obtain permission prior to accessing learning materials from unapproved sources.
- Not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- Not share any passwords with pupils, staff or third parties unless permission has been sought from the headteacher.
- Not install any software onto your device unless approved by Agilisys or headteacher.

- Ensure your device is protected by anti-virus software installed by Agilisys and that this is checked on a termly basis.
- Not use your device to take images or videos of pupils, staff or parents unless permission has been granted from the headteacher.
- Not store any images or videos of pupils, staff or parents on your device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, only process images or videos of pupils, staff or parents for the activities for which consent has been sought.
- Not use your device to communicate with pupils or parents, unless permission has been sought from the headteacher.
- Not use your device to send any inappropriate messages, images or recordings.
- Only access social media sites as approved by the headteacher on your device, and ensure they are used in accordance with the Technology Acceptable Use Agreement.
- Allow Agilisys to monitor your usage of your device, such as internet access, and understand the consequences if you breach the terms of this agreement.

Insurance cover provides protection from the standard risks whilst a school-owned device is on the school premises or in your home but excludes theft from your car or other establishments. Should you leave a school device unattended and it is stolen, you will be responsible for its replacement and may need to claim this from your insurance company or pay yourself.

Failure to agree to, or abide by, these terms will lead to the school device being returned to the school and serious breaches may result in disciplinary action.

Please complete this section if you are using a personal device for work purposes.

If you wish to use a personal device for work purposes, you must provide your consent below to allow Agilisys to access to your device and personal information, to conduct routine security checks and prevent the loss of any data. If you fail to provide this consent, you will no longer be permitted to use your personal device for work purposes including, but not limited to, accessing the online portal, school systems or work email accounts.

I understand the risks posed to my personal information when using a personal device for work purposes and confirm that I will be using a personal device at work. By signing below, I am providing consent for my device to be accessed for security checks and understand how my personal information could be affected.

Signed: _____ Date: _____

Print name: _____

I certify that I have read and understood this agreement and ensure that I will abide by each principle.

Signed: _____ Date: _____

Print name: _____ Device model and number: _____

Headteacher

Signed: _____ Date: _____

Print name: _____

Appendix 3: Remote Learning Plan 2020 - 2021

Rationale
At St Michael's, we are committed to providing continuity of education for our students in the event of individual student absence, partial school closure, e.g. form groups, or a whole school closure. We will operate a blended learning approach consisting of face-to-face learning for those students in school; distance learning provision for whole form/year groups who are unable to attend school and independent work for individual students who may be absent from a year group.

Students will be in receipt of a broad and balanced curriculum and be provided with suitable learning activities that are ambitious, supporting their progression. While such situations are inevitably highly varied in their causes and ramifications, we will endeavour to provide continued learning for our students during any period of closure in the following ways:

- The provision of high quality, relevant, learning activities for each subject area, ensuring students read, write, solve problems and have appropriate assessment points. All activities will be meaningful and ensure that students still have the opportunity to progress when they are actively engaged with our provision.
- Regular, live instruction from staff, with the ability for students to ask questions of their teachers in real time; this could be via the Google Classroom, Microsoft Teams (video lessons) or school email.
- The opportunity for students to have work assessed by their teachers and receive feedback. Subject leaders will determine the best way to feedback to students regarding their particular subject area.

All work set and submitted for assessment will be made available and distributed electronically. Work will be set, submitted for assessment, and assessed through the Google Classroom. The platform allows work to be set in a variety of formats e.g. presentations, videos and diagnostic quizzes. Students can access their work and complete it on the platform without needing printing facilities at home. Students can submit their work via the platform and teachers can give feedback to students on individual pieces of work. The Read and Write package that we have enables those students who need support with reading and writing to access their work; teachers and learning support practitioners will also support with this.

All staff and students have been set up on Google Classroom and it will be the responsibility of teachers to add work accordingly. There is also an expectation for staff to broadcast live lessons using Microsoft Teams or via a video recording. All staff and students have been set up on Microsoft Teams.

Scenario 1: Individual remote learning
For instances where the school remains open but an individual student is unable to attend lessons as normal, despite otherwise being well and able to work (such as when in a-symptomatic self-isolation) the student will receive individual provision.

- The individual provision will be coordinated in the first instance by the Admin team (YW&NC) and supported by the Head of Year and Assistant Head of Year for that year group.
- YW will notify subject teachers of the student's absence and the subject teachers will then set appropriate learning activities via the Google Classroom platform. Heads of Year and Assistant Heads of Year will issue reminders and check that work has been set.

- The Head of Year/Assistant Head of Year will notify parents via appropriate means e.g. a telephone call or email that work has been set for the student.
- If absence of this nature continues for more than one week, additional work should be requested and provided on a weekly basis through the Google Classroom until the student is able to return to school.
- Any supplementary work such as homework and revision activities can also be posted on Google Classroom.
- In this instance, students will access their work via their specific class rather than as a year group.

Scenario 2: Partial closures for particular form groups/year groups
If circumstances prevail whereby form or year groups are not in school for their full timetable, teachers will ensure that live contact via the Google Classroom and Microsoft Teams will enable students to access their curriculum.

- Subject teachers will set work for their absent class via the Google Classroom. Video lessons will be in conjunction with the school timetable and be delivered on Microsoft Teams at the beginning of the timetables double period. Please see safeguarding procedures for distance education provision, section 11 of this policy.
- Subject teachers will set work for their absent class via the Google Classroom. Tasks will be the same/as similar as possible to what students would have being completing in school. Learning activities will be designed to last the equivalent amount of time as the subject's lessons and homework times during one calendar week. Assignments from each subject will be set immediately in the event that a partial school closure is announced, and students and parents will be notified of this by email. The Head of Department will quality assure work set and ensure that learning activities are appropriate and are in accordance with the curriculum map.

Scenario 3: Rota based system for Year groups (tier 2/3 closure)
This is now a highly anticipated situation. Our system enables students in school to receive face-to-face teaching as well as live delivery/learning provision for those students who are at home. Staff should expect to be working in school during a tier 2/3 closure.

- Students in school will receive face-to-face teaching.
- Subject teachers will set work for their absent class via the Google Classroom. Video lessons will be in conjunction with the school timetable and be delivered on Microsoft Teams at the beginning of the timetables double period. Please see safeguarding procedures for distance education provision, section 11 of this policy.
- Subject teachers will set work for their absent class via the Google Classroom. Tasks will be the same/as similar as possible to what students would have being completing in school. Learning activities will be designed to last the equivalent amount of time as the subject's lessons and homework times during one calendar week. Assignments from each subject will be set immediately in the event that a partial school closure is announced, and students and parents will be notified of this by email. The Head of Department will quality assure work set and ensure that learning activities are appropriate and are in accordance with the curriculum map.

Scenario 4: Longer-term closures for the whole school

If circumstances prevail whereby the whole school has to close for a period longer than 5 working days, students will access their curriculum via distance learning provision.

- In the event that the whole school is closed, we will move to a model by which subject departments will set work for classes on the Google Classroom. Students will work at home following their usual school timetable if possible (this is flexible dependent upon individual situations). Work will be set in conjunction with school timetables and students will be supported via contact through the Google Classroom platform, school email or the live chat function on Microsoft Teams.
- Live lessons/video lessons will be delivered via Microsoft Teams to supplement learning tasks set on the Google Classroom. Video lessons will be in conjunction with the school timetable. Please see safeguarding procedures for distance education provision, section 11 of this policy.
- Instructions for learning will be posted on the Google classroom, and explained during the live lesson/video broadcast delivery. Learning journeys/road maps will be used to show curriculum sequencing in all subjects.
- The school reserves the right to vary the methods described in whatever way they feel is best for the students.
- For all year groups, learning tasks will be set per year per subject to cover their lessons for that particular week including additional time for weekly homework.

Lesson provision

Students are expected to work on learning activities tasks during the week in which they are set in correspondence with their school timetable. Work will correspond to curriculum maps and where possible be the same activities that they would be doing in school. During this time, teachers are expected to have an online presence via Google Classroom at the time they would normally have a lesson with that year group to be available for students to ask questions in real time. There is an expectation for staff or students to broadcast audio or video using Microsoft Teams This software has effective functionality for online lessons without a time limit. Students will be expected to take part in the live sessions that are available if they are well enough to do so. Lessons will be recorded so that students can access the lesson at a different point. The live lesson/video aspect of the lesson will last approximately 25 minutes. The remainder of the lesson will be spent completing work on the Google Classroom. Lesson activities will be as close to in-school learning activities as possible. Some departments may provide links to alternative sites, for example, the Maths department will set work via Hegarty maths. All students have login details for this and if they have any difficulties, can contact their Maths teacher for support. Any live contact with teachers can still happen via the Google Classroom or email.

Where possible, support will be live, but with a multitude of scenarios that could be taking place at home for both students and staff this may not always be possible. If support is not immediate or during the designated lesson time, queries and support will be provided in a timely manner.

Expectations of students

Assuming that students are well enough to work, students are expected to:

- complete all work set for them and submit work which is requested for feedback promptly by the assignment deadline date
- check emails and Google Classroom notifications regularly and read and respond if necessary to communications from the school
- immediately inform teachers if they are having problems with the work. Students must reach out for support if needed

- ensure that they have access to a laptop/tablet/phone and inform their Heads of Year immediately if not
- where students experience problems with IT systems they should proactively inform Agilisys by emailing stmichaels.it@sgilisys.co.uk
- students are expected to uphold the same standards of conduct and behaviour during live online lessons as they would be expected to in school
- ensure full engagement with the tasks in hand, including submission of any required work by the deadline that has been set
- ensure that clothing is appropriate, following the same guidance as normal "Non uniform" day in school if attending a video lesson
- access weekly learning plans to ensure clarity of instruction

Expectations of Staff
Assuming staff are well enough to work and have not called YW following the standard absence procedures, staff are expected follow the expectations below.

- Ensure that work is set to and made available on the Google Classroom at the start of each week to cover the calendar week ahead, and that sufficient resources are made available to students via electronic means to allow them to carry out work at home. Where textbooks are not available online, staff should, at the very least, scan relevant pages and share them with students along with the resources for that week's lesson.
- Provide a 25-minute live broadcast/video to students, providing clear explanations for students.
- Subject leaders coordinate the setting of work in the event of a whole school closure. They will delegate accordingly, in order to achieve a streamlined approach for each year group.
- Whole year group tasks will be set for years 7-9. Individual class teachers are responsible for their classes in Year 10 and 11. Subject leaders will quality assure and oversee this.
- To be familiar with the use of Microsoft Teams, and be available online through Teams at the times that they would usually have lessons to engage in live support with their students.
- LSPs will support students in a variety of ways depending on the given scenario. This could involve participating in live lessons and fielding questions, supervising vulnerable or key worker children and providing tailored support for those students with specific needs.
- ensure students receive feedback in line with departmental expectations – moved from student section

If there are reasons other than your own personal illness that will cause difficulties with you being live in front of a class at the timetabled time, you will need to contact your line manager in the first instance to discuss how this can be resolved.