ST MICHAEL'S
Church of England High School

IT 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:

Appendices

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 IT plays an important part in both teaching and learning over a range of subjects.

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.

This policy covers the rules and procedures for authorised and unauthorised use of the IT and communication facilities and is implemented in conjunction with the school's E-safety Policy.

Signed by:

_____ Headteacher Date: _____

_____ Chair of governors Date: _____

Date adopted 26th November 2015
Date revised 18th October 2017
Next revision date January 2021

1. Overview

1.1. The IT facilities at St Michael's Church of England High School are defined as:

- computers and software
- monitors
- keyboards
- computer mice
- printers
- scanners
- cameras
- camcorders
- other devices including furnishings and fittings used with them
- The communication facilities at St Michael's Church of England High School are defined as:
    - telephones
    - fax machines
    - televisions
    - video players
    - DVD players
    - satellite receivers
    - mobile phones
    - projectors
    - display screens
    - other devices including fittings used with them
    - Internet and e-mail can be defined as a communication facility used in conjunction with IT facilities; as such, these will coincide with the IT facilities.

1.2. This policy contains:

- the school's view on the use of e-mail and the internet at work
- an explanation on what you can or cannot do
- the consequences if you fail to follow the rules set out in this policy
- general information relating to IT, including the Data Protection Act
- how the policy is implemented
- the Managed Service Provider's duties to the IT policy

2. Policy

2.1. The use of the IT facilities within the school is encouraged, as its appropriate use facilitates communication and can improve efficiency.

2.2. Used correctly, it is a tool that is of assistance to employees. Its inappropriate use, however, can cause many problems, ranging from minor distractions to exposing the school to financial, technical, commercial and legal risks.

2.3. Staff should always be an example of good practice to the students, serving as a positive role model in every aspect.

2.4. Abuse of the IT facilities could result in the facilities being removed. Staff should always be aware of IT use, and misuse of the facilities, as defined in this policy, must be reported to the Headteacher.

2.5. Students are bound by the Acceptable Use Policy.

2.6. Staff should make sure that pupils comply with that policy.

2.7. Students misusing the IT facilities must be reported to the Headteacher.

2.8. This policy applies to any computer connected to the school's network and computers.

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

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

3. Procedure

3.1. The school's e-mail system and internet connection are available for communication and use on matters directly concerned with school business.

3.2. Employees using the school's e-mail system and internet connection should give particular attention to the following points in this policy.

3.3. E-mail should not be used as a substitute for face-to-face communication, unless it is otherwise impossible.

3.4. "Flame-mails" (e-mails that are abusive) can be a source of stress and can damage work relationships.

3.5. Hasty messages, sent without proper consideration, can cause unnecessary misunderstanding.

3.6. If an e-mail is confidential, the user must ensure that the necessary steps are taken to protect confidentiality.

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

3.8. The school's e-mail system and accounts must never be registered or subscribed to unsolicited e-mail (SPAM).

3.9. Never disclose any of the school's e-mail addresses without confirming that they will not be subjected to SPAM and that they will not be sold on to marketing companies.

3.10. All e-mails that are sent or received must be retained within the school for a period of six months.

3.11. All e-mails being sent to external recipients must contain the school's address and the direct contact details of the sender.

3.12. Non-text e-mails (containing graphics or colour) and e-mail attachments may contain harmful materials and computer viruses, which can seriously affect the IT facilities. If unsure, seek assistance or approval from the Managed Service Provider.

3.13. Offers or contracts sent via e-mail or the internet are as legally binding as those sent on paper. An exchange of e-mails can lead to a contract being formed between the sender, or the school, and the recipient. Never commit the school to any obligations by e-mail or the internet without ensuring that you have the authority to do so. If you have any concerns, contact the Headteacher.

3.14. Online purchases are only permitted with the Headteacher present, in order to comply with monitoring and accountability. Hard copies of the purchase must be made, for the purchaser and the Business Manager - Finance. This is in addition to any purchasing arrangement followed according to school policy.

3.15. Any failure to follow these procedures satisfactorily may result in disciplinary action, including summary dismissal.

4. Authorised use of the IT facilities

4.1. The IT facilities should only be used as required by your work duties. This includes, but may not be limited to:

- preparing work for lessons, activities, meetings, reviews, etc.
- researching for any school related task
- any school encouraged tuition or educational use
- collating or processing information for school business
- personal e-mail accounts are only permitted to be used if they have built-in anti-virus protection approved by the Managed Service Provider. Access to your personal e-mail must never interfere with your work duties.

5. Authorised use of the communications facilities

5.1. The communication facilities should only be used as required by your work duties. This includes, but may not be limited to:

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

5.2. If unsure about your required use, please seek authorisation from the **Headteacher**.

6. Unauthorised use of the IT facilities

6.1. It is not permitted under any circumstance to:

- use the IT facilities for commercial or financial gain without the explicit written authorisation from the Headteacher
- physically damage the IT facilities
- re-locate, take off-site, or otherwise interfere with the IT facilities without the authorisation of the Assistant Headteacher Facilities and Resources or Headteacher. Certain items are asset registered and security marked; their location is recorded by the financial assistant for accountability. Once items are moved after authorisation, staff have a responsibility to notify the financial assistant 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 IT 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. This is illegal under the Computer Misuse Act.

6.2. Use the IT 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
- remarks relating to a person's sexual orientation, gender assignment, religion, disability or age
- 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

6.3. Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.

6.4. Install hardware or software without the consent of the Assistant Headteacher Facilities and Resources, the Managed Service Provider or the Headteacher.

6.5. Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the IT facilities or that will bypass, over-ride, or overwrite the security parameters on the network or any of the school's computers. This is illegal under the Computer Misuse Act.

6.6. Use or attempt to use the school's IT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.

6.7. Purchase any IT facilities without the consent of the Assistant Headteacher Facilities and Resources or the Headteacher. This is in addition to any purchasing arrangements followed according to school policy.

6.8. 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.

6.9. Use any chat-lines, bulletin boards or pay-to-view sites on the internet. In addition, you must not download or attempt to download any software.

6.10. 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 school policy.

6.11. 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.

6.12. Use the IT facilities for personal use without the authorisation of the Headteacher. This authorisation must be requested on each occasion of personal use.

6.13. Copy, download, or distribute any material from the internet or e-mail 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.

6.14. To obtain and post on the internet, or send via e-mail, any confidential information about other employees, the school, its customers or suppliers.

6.15. Interfere with someone else's use of the IT facilities.

6.16. Be wasteful of IT resources, particularly printer ink, toner and paper.

6.17. Use the IT facilities when it will interfere with your responsibilities to supervise students.

6.18. Any unauthorised use of e-mail or the internet is likely to result in disciplinary action including summary dismissal.

6.19. If you are subjected to, or know about harassment or bullying, you are encouraged to report this immediately to your line senior or the Headteacher.

7. Unauthorised use of the communications facilities

7.1. It is not permitted under any circumstance to:

- use the communication facilities for commercial or financial gain without the explicit written authorisation from the Headteacher
- physically damage the communication facilities
- use the communication facilities for personal use without authorisation from the Headteacher with the exception of the circumstance in 7.2
- re-locate, take off-site or otherwise interfere with the communication facilities without the authorisation of the Headteacher

7.2. Use the communication facilities at any time to access, receive, view or display any of the following:

- any material that is illegal
- any material 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
- remarks relating to a person's sexual orientation, gender assignment, religion, disability or age
- 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 material
- any adult or chat-line phone numbers
- use or attempt to use the school's communication facilities to undertake any form of piracy, including the infringement of media rights or other copyright provisions whether knowingly or not. This is illegal.
- use or attempt to use the school's communication facilities for internet or e-mail 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.
- copy, record or distribute any material from or with the communication facilities that may be illegal. This can include television media, films, telephone conversations and music. 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.
- use the communication facilities when it will interfere with your responsibilities to supervise students.
- use of the school's telephone facilities for personal use is permitted for necessary calls lasting less than 10 minutes. Should you need to use the telephones for longer than this, then authorisation must be sought from the Headteacher. This authorisation must be requested on each occasion. The exception to authorisation is the use of the telephone system to make personal emergency calls. However, the duty head or Headteacher must be notified after the call. Any personal use of the telephones may be subject to a charge; this is at the Headteacher's discretion.

7.3. All items are asset registered and security marked; their location is recorded by the financial assistant for accountability. Once items are moved following authorisation, staff have a responsibility to notify the financial assistant of their new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.

7.4. If you are subjected to or know about harassment or bullying, you are encouraged to report to your line senior or Headteacher.

8. Implementation of the policy

8.1. Staff are requested to report any breach of this policy to the Headteacher.

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

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

8.4. Use of the school's internet connection is recorded and monitored.

8.5. The financial assistant randomly checks asset registered and security marked items.

8.6. The Managed Service Provider checks computer logs on the school's network regularly.

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

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

8.9. The Managed Service Provider can remotely view or interact with any of the computers on the school's network. This may be used randomly to implement the IT Policy and to assist in any difficulties.

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

8.11. The school's database systems are computerised. Unless your line manager gives you express permission, you must not access the system. Failure to adhere to this requirement may result in disciplinary action.

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

8.13. 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.

8.14. User accounts are accessible by the Headteacher and the Managed Service Provider.

8.15. 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.

8.16. Users are required to be familiar with the requirements of the Data Protection Act 1998 and, from 25th May 2018, the General Data Protection Regulation and to ensure that they operate in accordance with the requirements of the Act. The obligations under the Act are complex but employees must adhere to the following rules:

- do not disclose any material about a person, including a pupil, without their permission
- such material includes information about a person's racial or ethnic origin, sex life, political beliefs, physical or mental health, trade union membership, religious beliefs, financial matters and criminal offences
- do not send any personal data outside the UK

9. Storing messages

9.1. Messages should be deleted after six months or stored in a suitable hard copy file.

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

9.3. If unsure, please seek help and information from the Assistant Headteacher Facilities and Resources and/or the Managed Service Provider.

9.4. Employees who feel that they have cause for complaint as a result of e-mail communications should raise the matter initially with their line manager or Headteacher, as appropriate. The complaint can then be raised through the grievance procedure.

10. The Third Party IT Managed Service Provider duties

10.1. To monitor and affect accountability of the IT policy, the Managed Service Provider is required to:

- carry out daily checks on internet activity of all user accounts and to report any inappropriate use to the Headteacher
- monitor the computer logs on the school's network and to report any logged inappropriate use to the Headteacher
- remotely view or interact with any of the computers on the school's network. This may be done randomly to implement the IT policy and to assist in any difficulties

- access files and data to solve problems for a user, with their authorisation. If an investigation is requested by the Headteacher, authorisation from the user is not required
- adjust access rights and security privileges in the interest of the protection of the school's data, information, network and computers
- disable user accounts of staff that do not follow the policy, at the request of the Headteacher
- assist the Headteacher in all matters requiring reconfiguration of security and access rights and in all matters relating to the IT Policy
- assist staff with authorised use of the IT facilities, if required

11. Policy review

11.1. This policy is reviewed every two years by the Assistant Headteacher – Facilities and Resources and the Headteacher.

11.2. The scheduled review date for this policy is March 2020.

Appendix 1: Technology acceptable use agreement

Name of school: St Michael's Church of England High School

Date:

Whilst our school promotes the use of technology, and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly, and will be reported to the headteacher 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 the school premises, and applies to all staff, volunteers, contractors, and visitors.

Please read this document carefully, and sign below to show you agree to the terms outlined.

1. **Using technology in school**

- I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use by the headteacher.
- I will only use the approved email accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information.
- I will not share sensitive personal data with any other pupils, staff, or third parties.
- I will ensure that any personal data is stored in line with the Data Protection Act 1998.
- I will delete any chain letters, spam, and other emails from unknown sources without opening them.
- I will ensure that I obtain permission prior to accessing learning materials from unapproved sources.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload, or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with pupils, staff, or third parties unless permission has been given for me to do so.
- I will not install any software onto school ICT systems unless instructed to do so by the data protection officer or headteacher.
- I will only use recommended removable media, and will keep this securely stored.
- I will provide removable media to the data protection officer for safe disposal once I am finished with it.

2. Mobile devices

- I will only use school-owned mobile devices for educational purposes.
- I will only use personal mobile devices during out-of-school hours, including break and lunch times.
- I will ensure that mobile devices are either switched off or set to silent mode during school hours and will only make or receive calls in specific areas, e.g. the staffroom.
- I will not use mobile devices to take images or videos of pupils or staff – I will seek permission from the headteacher before any school-owned mobile device is used to take images or recordings.
- I will not use mobile devices to send inappropriate messages, images, or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the WiFi system using personal mobile devices, unless permission has been given by the Headteacher or Assistant Headteacher, Facilities and Resources.
- I will not use personal and school-owned mobile devices to communicate with pupils or parents.
- I will ensure that any school data stored on school or personal mobile devices is password protected, and give permission for the Assistant Headteacher, Facilities, and Resources to erase and wipe data off my device if it is lost or as part of exit procedures.

3. Social media and online professionalism

- If I am representing the school online, e.g. through blogging, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access social networking sites, unless it is beneficial to the material being taught; I will gain permission from the Headteacher before accessing the site.
- I will not communicate with pupils or parents over personal social networking sites.
- I will not accept 'friend requests' from any pupils or parents over social networking sites.
- I will ensure that I apply the necessary privacy settings to my social networking sites.
- I will not publish any comments or posts about the school on my social networking sites, which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

4. Training

- I will ensure I participate in any e-safety or online training offered to me, and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the Assistant Headteacher, Facilities and Resources to undertake regular audits in order to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- I will ensure that I deliver any training to pupils as required.

5. Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the **E-Safety Policy**, e.g. to monitor pupils' internet usage.
- I will ensure that I report any misuse by pupils, or by staff members breaching the procedures outlined in this agreement, to the Headteacher.
- I understand that my use of the internet will be monitored by the Assistant Headteacher, Facilities and Resources and recognise the consequences if I breach the terms of this agreement.
- I understand that the Headteacher may decide to take disciplinary action against me in accordance with the Allegations Against Staff Policy, if I breach this agreement.

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

Signed: _____ Date:_____

Staff Member

Print name:_____

Signed: _____ Date:_____

Headteacher

Print name:_____