ST MICHAEL'S
PREPARATORY SCHOOL

ICT Acceptable Use Policy

Review Date: July 2024
Latest Review Due: July 2025
Staff responsible: Mr Gareth Green (Assistant Head Academic)
Chair of Governors: Mark Taylor

This policy should be read in conjunction with the following St Michael's policies:

- *Safeguarding Policy*
- *Staff Handbook (for staff)*
- *Data Protection Policy*
- *Privacy Policy*
- *Anti-bullying Policy*

Introduction

This policy outlines the acceptable use of Information and Communication Technologies (ICT) at St. Michael's School. A copy of this document can be accessed on the school website. At St. Michael's, we prioritise the safety and responsible use of information technology. In today's digital world, it is crucial to establish clear guidelines and protocols to ensure a secure and productive environment for our students, faculty, and staff.

ICT is not just about computers. ICT in the EYFS and KS1 is taught both as an integral part of the curriculum as well as through a distinct lesson in KS1. In EYFS pupils work towards the Early Learning Goals in the 'Technology' strand of the 'Understanding of the World' section and are given a broad, play-based experience of ICT in a range of contexts, such as role play. These skills develop throughout the Nursery, Reception, Year 1 and 2 experience in school and by the end of Key Stage 1 pupils are taught about programming using logical reasoning to predict, write and test the behaviour of simple programs. All pupils should be taught through discussion throughout their time in school to communicate safely and respectfully online, keeping personal information private and recognising common uses of IT beyond school.

With this goal in mind, we have developed a comprehensive policy that covers general ICT use and the specific utilisation of Chromebooks and iPads, divided into two parts. Pupils in EYFS and KS1 ensure that IT digital safety is discussed at the start of each academic year. Where appropriate, pupils are encouraged to sign a code of conduct document to demonstrate they understand the importance. Teachers use their discretion in their choice of and use of the correct information and documentation.

Part One - General ICT Use (Appendix One)

Appendix One focuses on the general expectations and guidelines for the safe use of information technology. At the start of each new academic year, these expectations are

shared with all students in Year 3-Sh. For students who join mid-year, their Form teachers explain the principles and guidelines. All students at St. Michael's are expected to read and sign Appendix One.

Part Two - Chromebook Program (Appendix Two)

Appendix Two outlines the expectations and guidelines specific to our 1:1 Chromebook program. Students in the Senior School, who are part of the Chromebook 1:1 scheme, are required to read and sign Appendix Two. Similar to new students entering mid-year, those students also receive a detailed explanation of the principles and guidelines from their Form teachers before signing the Pupil Pledge.

By adhering to this policy, we aim to equip our community with the necessary skills and knowledge to responsibly navigate the digital landscape. We strive to foster a culture of digital citizenship, ensuring a positive and enriching educational experience for all.

Monitoring

Use of ICT is monitored and filtered within the school, and cases of misuse by staff and pupils will be reported to the Head. A log of any incidents is kept on file. This policy will be reviewed annually, and action taken if a need for change is identified.

Where our filtering system detects attempts to access websites or materials considered to present a risk of harm (including, but limited to intolerance, racism, terrorism and self-harm) will automatically generate an alert via the Lightspeed filtering system that will be sent to the School's DSL and IT technician). The school may also share our filtering reports with external services to help us identify inappropriate or safeguarding issues. Please read our Safeguarding and Child Protection Policy for more information.

Technology in Education and Digital Safety

St. Michael's School acknowledges the vital role of technology in education, but also recognises the importance of balancing digital engagement with traditional learning methods. While encouraging students to develop essential IT skills, the school advocates for a balanced approach to learning, ensuring that students benefit from both the dynamic possibilities of digital tools and the enduring value of written work and traditional paper-based text.

To implement this balanced learning approach, St. Michael's integrates ICT thoughtfully across the curriculum. In Early Years Foundation Stage (EYFS) and Key Stage 1 (KS1), technology is incorporated into various subjects and taught as a discrete lesson in KS1. Students are gradually introduced to technology through play-based activities, progressing to programming and coding by the end of KS1. In Key Stage 2 (KS2) and Key Stage 3 (KS3), **IT digital safety**, **responsible IT usage**, and **cybersecurity** are taught in IT lessons. Throughout their time at St. Michael's, students are encouraged to discuss and understand

the importance of online safety, privacy, and respectful digital communication. This measured integration of ICT aims to cultivate a well-rounded learning experience encompassing digital literacy alongside traditional academic skills.

In addition to dedicated IT lessons, digital safety is also a key component of the Personal, Social, Health, and Economic (PSHE) education curriculum. Through PSHE lessons, students explore various aspects of online safety, responsible digital citizenship, and strategies for navigating the digital world responsibly and safely. St. Michael's School also recognizes the crucial role parents play in supporting their children's digital well-being. The school hosts an **annual presentation on e-safety for parents**, providing them with valuable insights, resources, and guidance to help them create a safe and positive online environment for their children.

Communication with parents

Parents are contacted directly where concerns exist regarding improper use of the Internet or school's ICT equipment. Improper use may result in pupils being banned from using systems and other disciplinary measures may be taken depending upon the nature of the abuse (e.g. Exclusion from school). All misuse and IT related issues will be dealt with under the school Behaviour Policy.

<u>All</u> emails/communication/documents/etc. must be thought through and professionally worded.

Guidelines for staff

Any school computer equipment or service utilised by a member of staff is provided for the primary purpose as a work tool, for work related duties only. It must not be used to conduct a personal business/enterprise for personal gain or to access/store any information/media/photos/files that could be seen to be inappropriate on the device. Any electronic communication with other members of the school must be made using the internal school systems taking into account that all communication/files must be of a professional nature.

Staff must keep their passwords secure and make sure their passwords are of significant strength. Passwords must not be given to any other members of staff or pupils at any time and care must be taken when typing in passwords to a device/computer/laptop to make sure that no other person can identify the password or pin code.

Staff are responsible for the security and acceptable use of their laptop/device/network account. Staff must ensure that their laptop and other computer equipment is stored securely when not in use. Staff must not keep passwords with their laptop. If a laptop is lost or stolen, a report must be made to the IT department and then, if necessary, the Police. Staff must provide the Police with a phone number for the IT department so that the equipment's serial number can be provided. The IT department must be provided with the crime reference number for insurance purposes.

Staff are expected to maintain reasonable care with all portable equipment. This includes taking measures to ensure that the equipment is transported in a safe and secure manner. Staff must not keep 'personal information' about pupils on their laptops in case of theft – data such as contact details etc. should not be stored on laptops.

All software should be installed by the IT department and must have the relevant licence made available to them before installation. Software without the correct licence must not be installed and staff who attempt to install software themselves will be responsible. With mobile devices and Apps if you require a password to install the app this must be carried out by the IT department (some devices may be unlocked to allow you to undertake this yourself). Online learning systems should be approved by the IT department before being purchased or set up.

The IT department maintains a software audit, containing a list of the software installed on each computer or laptop. This audit will be made available to any official body who require it for the purposes of copyright enforcement. The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licences must always be adhered to.

The copying of music files, video and other copyright material if not legally purchased by the member of staff/pupils onto school computers may be illegal and removed if discovered. DVD's may only be played to an audience if it is within the terms of their licence agreement or the school holds an additional licence which allows. School mobile devices may be locked to not allow such content in which case no member of staff should circumvent this setting.

Whilst it is the user's responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above must contact the IT department who will assist in resolving any issues.

The school has the right to seize/reclaim any laptop or computer without explanation.

The IT department has the ability to view all files on the network and devices but are prohibited from doing so without permission from the Headteacher, Chair of Governors or the Office Manager.

Staff are responsible for backing up data when they end their employment with the school. Staff must be aware of the Data Protection Act and are prohibited from taking copies of any personal data about pupils or other members of staff.

Data Protection

Data is stored in accordance with the regulations laid out by the Data Protection Act. We will take every reasonable precaution to protect information. Appropriate physical, electronic and procedural safeguards are in place to ensure the security, integrity and privacy of all information kept in our MIS. The need for confidentiality will be respected,

and sharing of data will only occur with the express permission of parents/carers in line with our fair processing notification. Please read our Data Protection Policy for more information.

Internet Safety

Internet safety skills are taught throughout the school, from Nursery to Shell. Senior Pupils are made aware through lessons in PSHE of their rights and responsibilities with regard to their use of technology. This includes issues such as cyber bullying, personal safety, data security and sexting. Pupils receive follow up guidance via their lessons, assemblies, focus weeks and external visitors/briefings.

Appendix One

ICT ACCEPTABLE USE POLICY: General use (pupils)

1. **These rules apply to all equipment.**
I know that these rules will apply to me at all times when I am using either provided ICT equipment in school, any equipment at home, or my own ICT equipment within school, such as computers, cameras, scanners, software and networks.

2. **Take care when using equipment.**
I will take care when I am using all ICT equipment. I will not break or damage any ICT equipment and if anything gets broken then I will report it straight away.

3. **Ask before using your own ICT equipment.**
I will not bring my own ICT equipment with me unless I have been given permission by a designated member of staff. If I am allowed to bring my own ICT equipment then I will obey all the

extra rules I will be given about how I can use it.

4. **Keep passwords safe.**
I will always log on using my own user-name and password. I will not tell my login details to anybody else. I know that I will be responsible for everything that is done using my login details. If I think that somebody else knows and has used my login details then I will report it straight away so that my login details can be changed.

5. **Nothing is secret.**
I realise that my use of both my own and provided ICT equipment will be monitored and that everything I do may be recorded. I agree that I have no right to privacy and I agree to being monitored and recorded at all times. I realise that the results of this monitoring may be shared with other people if I break any of the rules.

6. **Keep personal information safe.**
I will not disclose any of my personal details to other people, or log any personal details on websites, while using ICT. (Personal details include telephone numbers, addresses and all types of personal financial information.) I agree that I will never pass on the personal details of another person without that person's permission.

7. **Understanding copyright.**
If I am downloading music, video or images, I will check with staff that it is legal and copyright free. I understand that music and video files are often put on the Internet illegally and that by using those files I will be breaking the law.

8. **Educational uses only.**
My use of ICT equipment will only be for educational uses, although limited personal use is permitted provided that this is not done during normal working time and does not contravene any of the other rules in this document.

9. **No hacking.**
I will not try to access any websites, services, files or other resources that are blocked or which I am not allowed to try accessing.

10. **Unsuitable material.**
I agree that I will not try to view, send, upload or download material that is unsuitable for viewing. If I accidentally see any unsuitable material then I will immediately close (but not delete, in the case of emails) the material and tell a member of staff. I know I will not be held responsible if I view unsuitable material by accident and I realise that by reporting this I will help to improve the e-safety of my school. If I am in any doubt about the suitability of any material, or if any doubts are raised, then I will not (re)access the material. I will not access material that has been rated as "unsuitable".

11. **Be polite.**
Proper conduct must be maintained at all times while using ICT. I agree that I will not harass, bully, insult or attack others via email or any other means. The use of strong language, swearing or aggressive behaviour is not acceptable. I will be polite at all times.

12. **Friends on Social Networking Sites.** School staff and pupils must not be friends on social networking websites. Furthermore, staff must not have School parents as friends, unless the staff member is also a parent within the school.

ST MICHAEL'S
PREPARATORY SCHOOL

13. **Photocopying.** I will try to reduce costs by only printing what I require. I will ensure that I check carefully whether I am printing in Colour or Black & White. I will ensure that I use the PC Client application and not send work directly to the printer.

14. **Using Shared Equipment.** When using shared IT equipment, I will respect the fact that other users will want to use it also. I will therefore ensure that I leave the equipment in a tidy order and on charge if applicable.

I realise that any contravention of the rules set out in this document may result in sanctions being applied. If I break any of these rules then my use of ICT in my school project(s) may be limited or completely stopped. My activities may also be reported to other people.
The schools response to 'out of school' social media posts will be in line with accepted good practice. St Michael's will investigate and take appropriate action to protect pupils who receive inappropriate communication from other St Michael's pupils via social media or online platforms, even when the communication takes place outside of school hours on non school devices. Cyberbullying and unpleasant social media communication between pupils has an impact on school life, friendships and playground conversations and therefore the school has a duty of care to investigate incidents that are brought to our attention.

Parents will be informed when these issues occur, if their child is involved.

Signatures:

Date:

Appendix Two

Chromebook Acceptable Use Policy for St. Michael's School

At St. Michael's, we are lucky to have our own Chromebooks to help us learn better with technology. It's important to follow some simple rules to make the most of these great tools. Please read and tick off each rule after you understand it.

Student Pledge for Chromebook Use

ST MICHAEL'S
PREPARATORY SCHOOL

Take Care of Your Chromebook:

Keep your Chromebook safe in your bag where it won't get wet or crushed. Do not throw or drop your bag as it may damage your Chromebook.

Report Problems:

Tell a teacher right away if your Chromebook is lost or damaged.

Bring It to School Charged:

Make sure your Chromebook is at school every day and fully charged.

E-Safety:

Use the internet safely. Don't send mean messages and tell a teacher if you see something upsetting online.

Use It Right:

Only use your Chromebook for schoolwork and only use apps and websites that are okay for school.

Keep It to Yourself:

Don't let others use your Chromebook and don't use someone else's. Don't share passwords

Food and Drink Free Zone:

Keep snacks and drinks away from your Chromebook to avoid spills.

No Repairs:

Don't try to fix your Chromebook yourself. Let the experts handle it.

Privacy Matters:

Ask for permission before taking photos of people.

Use Features Wisely:

Only use the camera and microphone when your teacher says it's okay.

ST MICHAEL'S
PREPARATORY SCHOOL

End of Year Reset:

Remember to save your important files to Google Drive before the end of the year reset.

Plagiarism and AI Use:

Do not copy others' work and claim it as your own. Using AI to do your schoolwork without permission is not allowed.

By following these rules, you help make our school a better place for learning. If you don't follow these rules, there might be consequences like getting a warning or even losing your Chromebook privileges.

The school keeps a Chromebook 'Tracker'. Should you misuse your Chromebook, not bring it into school or not bring it in fully charged, this will be recorded on the Tracker. Should three incidents be recorded, a warning will be issued. The Chromebook Tracker resets each term.

I agree to follow these rules and understand the consequences if I don't.

Signed: _____ Date: _____