The St Marylebone Church of England School
64 Marylebone High Street
London W1U 5BA

ICT ACCEPTABLE USE POLICY (Pupils)

Author:	**Susan Anderson**
Link SLT:	**Susan Anderson**
Review Governor:	**Emma Rea**
Last reviewed:	**January 2020**
Next review date:	**2022/23 (every 3 years)**
Approval at Plenary Required:	**Yes**
Required to publish on website?	**No**
Statutory:	**No**
Committee:	**Staffing and Management**

1. Context

The aim of this policy is to set out safe and responsible behaviour when using ICT facilities at The St Marylebone CE School ("the School"). These facilities include computers, Chromebook, software, email, G Suite, the managed learning environment and internet access.

The School recognises and embraces the potential of technology to enhance teaching and learning. ICT equipment and services are provided in order to support the school community and make sure that everyone has access to the benefits of technology.

Our networked ICT facilities serve as a first line of defence in keeping users safe and secure. We use a range of security techniques, including anti-virus, internet filtering and email and network monitoring. Our managed service provider monitors all network use and can report back detailed information about each user's activity on the network.

Bearing this in mind, it is important that each user takes responsibility for their own use of technology, making sure that they behave safely, responsibly and legally and that they follow the e-safety advice and guidance provided. The school expects high standards of behaviour when using technology and will treat any breach of policy seriously.

2. Pupil responsibilities

1. You must learn to recognise and avoid risks online – to become 'Internet Wise'. To STOP and THINK before you CLICK, so that you can make good judgements about what you see, find and use.

2. You must be aware of your social responsibilities when using the internet and other communication technologies, so that you treat others with respect, and report any online bullying to an adult.

3. No form of technology or device, whether provided by the school or personally owned by you, may be used for the bullying or harassment of others in any form. Cyber-bullying is taken very seriously and will be dealt with in the same ways as any other kind of bullying.

4. You must not use any form of technology or service to bring the school, or its members, into disrepute.

5. You have a duty to respect the technical safeguards that are in place. Trying to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.

6. You have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others.

7. If you find that there are any failings in technical safeguards, it is your duty to report them so that the matter can be resolved.

8. If you access anything inappropriate or worrying by mistake, or you receive an email or text message that bothers you, you should not respond to it, but you should tell a responsible adult so that the matter can be resolved.

9. You have a duty to protect your password and personal network login, and you should log off the network when leaving computers unattended. You must use a strong password that is unique to your school account. If you access your email and google apps on a personal device, then this device must be security protected and your access to your account must be password protected on this device.

10. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable. You should only access the resources that you have permission to use.

11. You have a responsibility to protect the security and confidentiality of school data and networks at all times and should take care when transferring files and opening attachments in order to avoid introducing viruses or inappropriate material into the school.

12. The school does not allow the use of social networking in school as it has no way to keep you safe in these spaces. You must take responsibility for keeping yourself safe online, both in school and at home. Giving out personal details or agreeing to meet strangers you have met online puts you in danger.

13. All network activity and online communications are monitored, including any personal and private communications made via the school network. School email addresses are provided so that you have a safe and secure communication method. Commercial webmail is not advised for use in school as your safety and security cannot be guaranteed.

14. You should print responsibly in order to reduce environmental impact. All users are given a printing quota to encourage responsible use.

15. You should be aware of intellectual property and copyright. You should not simply copy and paste as plagiarism is not only cheating but where a sufficient amount is copied, this is an illegal infringement of copyright and is also a criminal offence.

3. Sanctions

1. Where unacceptable use is suspected, enhanced monitoring and reporting procedures may come into action, including the power to check and/or confiscate personal technologies such as mobile phones.

2. Most breaches of this policy will be dealt with through the school behaviour policy, which has sanctions that increase in response to the severity of the issue. Removal of internet privileges may also be imposed.

3. Any issues that involve illegal use of the ICT facilities, or where child protection is compromised will be reported to the police and/or relevant child protection agencies.

Further information on E-Safety policy

Think U Know: www.thinkuknow.co.uk

Know IT All: www.childnet-int.org

4. This policy should be read with reference to

4.1 The Anti-Bullying Policy

4.2 The Behaviour for Learning Policy

4.3 The E-Safety Policy