Summary of key policy guidelines:

- This policy applies to **all school computers and devices** and also **any mobile and tablet devices** that you use in school, and also to your **online behaviour** towards other Millfield users inside and outside of school.
- **Do not record sound, video, take photographs in lessons** on any device unless for an activity under the direction and permission of a supervising teacher. Do not upload online, share or broadcast any such content unless given specific permission by your teacher.
- Use of mobile devices in class is under the choice, permission and direction of the teacher.
- Electronic contact & discussions with your teacher **must be respectful and appropriate at all times** and must only be part of approved school activities.
- You must ensure that your mobile device for class use has sufficient storage capacity available for downloading school apps and performing educational activities.
- Protect our identities online by **not sharing passwords, not uploading personal details** of you or other Millfield users. Regularly check and review your privacy settings on online sites & accounts.
- **Accessing someone else's computer, phone or tablet or school/online accounts** without that person's permission is illegal.
- Always ensure that your mobile device, tablet device and any online accounts that you use have **passcodes switched on**, and that passcodes are not revealed or shared with others.
- **Do not upload or share images, video and other content** that is indecent or could embarrass or harass others, or could break the law.
- Report any suspicious online inappropriate approaches or threatening behaviour to **Head of Computing & ICT** or **Deputy Head (Pastoral)** at the Prep School. Report to your HP, teacher or **Deputy Head (Pastoral)** at the Senior School, and also to the authorities (CEOP) where appropriate.
- Do not publish or share any information that defames, undermines, misrepresents, or tarnishes the reputation of the school or its users.
- **Do not bully others online, and report any harassment or bullying to your HP or teacher.**
- Do not access unsuitable or inappropriate material online.
- **Back up** any important work by making a copy and storing it somewhere else that is safe.
- **Copying files** (images, music, video, text) that are copyright protected is against the law.
- Do not install software onto the school network, or try to circumnavigate any of the network and ICT controls that are in place.
- **The school may monitor your use of IT systems and online behaviour** to maintain safety and also compliance with this policy.

1. Use of Mobile Learning technologies and school WIFI

Use of pupil-owned tablet devices (iPads) to support teaching and learning activities is compulsory for pupils in Years 7 and above, and the content of this policy also applies to this use. Separate guidelines on classroom use of tablet devices (iPads) are issued to pupils and teachers. The school reserves the right to monitor, remove, reconfigure, and suspend use of pupil owned iPads and content to ensure compliance with this policy. The recording of sound, images or video in lessons by pupils is at the direction and permission of the supervising teacher. Do not upload online, share or broadcast any such content unless given specific permission by your teacher. Mobile devices should have passcodes set, 'find my iPad' (or similar) settings switched on, not be left out of sight and should be locked when not in use. Use of a mobile device in lessons is at the permission and direction of the supervising teacher. You must ensure that sufficient capacity is available on your mobile tablet device for school educational activities.

2. Protecting our identities online

Be aware that identity theft is an online danger that is increasing, and you should take precautions to prevent this happening. Do not upload or reveal your, your families or other Millfield users' personal details online (e.g. address, phone number, date of birth, financial details, passwords, etc.) Do not upload any images and/or comments that could embarrass you or other Millfield users and families – once uploaded it is often difficult or even impossible to remove such online content. Be aware that uploading digital photographs taken from a mobile device may reveal your precise GPS location at a given date and time, and therefore may reveal your movements and locations to those you would wish not to know. Avoid using your own photographs to identify yourself online, try to use an avatar or cartoon images instead.

3. Protecting yourself from Internet dangers

Report any suspicious or inappropriate approaches, messages or similar online behaviour to your parent, Group Tutor, Head of Year, House Parents, **Deputy Head (Pastoral)** or **Head of Computing & ICT** at MPS, and **Deputy Head (Pastoral)** at the Senior School; you may also report serious or urgent suspicions to the police by using the CEOP button available on many online chat & social networking sites, or seek help via the CEOP website. Do not store, transmit, or distribute any inappropriate or revealing images of yourself or others.

4. Use of chat, blogging and social networking facilities

These and similar facilities should be used safely, responsibly and not to excess, and should be accessed at times agreed by your supervising member of staff in accordance with school rules. You must not use offensive, derogatory, racist, sexist, unpleasant language comments/audio/imagery that could embarrass the school or its users, on any app, chat, blogging, e-mail, messaging, VLE or similar internal or external system. Please ensure that when using any such sites that your security and privacy settings are set to protect the safety and identity of you and your friends. Electronic contact with your teacher must be respectful and appropriate at all times, and must be only as part of approved school activities.

Where email or file cloud storage is used in relation to school activities, the school provided email address and storage must be used.

5. Online publication of Millfield-related information

You must not submit or publish information about Millfield School, or any of its users, or its logo unless part of an approved educational activity. This includes using apps, micro-blogging sites such as Twitter, blogging, social networking, personal web pages, VLE, e-mail systems, text, online forums & chat or any other web-based public information and collaboration systems, and any app service.

Where information relating to Millfield School or its members (staff or pupils) is to be published online, the content must not defame, undermine, misrepresent, or tarnish the reputation of the school or its users.

6. Online bullying

Using apps, e-mail, text, messaging, chat, VLE, social networking, blogging, or any other electronic method to send or publish offensive or untrue messages or post unpleasant comments/imagery that could intimidate, harm, or humiliate other Millfield users or their families, is forbidden and could also be breaking the law. This includes 'trolling'. (Please refer to the school anti-bullying policy and anti-cyber bullying policy).

7. Staying within the laws

What you do or say online is covered by a number of laws, and increasingly people are being prosecuted for offensive and illegal comments made by electronic communications, and on sites such as Twitter, and Facebook etc., so think before you post online or send. Unauthorised access to IT systems, accessing others' social networking accounts, e-mail accounts etc., without their permission is an offence under the Computer Misuse Act.

8. Personally owned computing & mobile devices

Regardless of the ownership of such devices (laptops, PDA's, Smart phones, tablets, digital cameras, mobile phones etc.) the school rules still apply to the use of such devices inside and outside of school where such use relates to Millfield School activity, and therefore the guidelines described within this document apply when such devices are being used. You must only use such devices in accordance with instructions from your teacher/houseparent, and in accordance with school rules.

9. Use of the Internet

Use of the Internet may be monitored where concerns have been raised, and a web-filtering system is in place. You must not access, store or share 'unsuitable' or illegal material on any school IT system or your own tablet or personal IT/telephony devices, or try to bypass our filtering or password security controls. Access to unsuitable content includes: gambling, pornography, promotion of bullying, proxy bypass sites, or sites inciting hatred of a particular group. Where internet access is gained outside of the school network e.g. via Mobile 3G/4G, the same rules apply in terms of not accessing 'unsuitable' material. Any access to unsuitable content, whether intentional or accidental, must be reported to the supervising member of staff and IT Services.

10. Logons

By logging onto the school network, your iPad, and any other school IT systems, you agree to the guidelines and policies for ICT use at Millfield School. You are responsible for any activity that takes place using your

school logon or any other password protected system. Your passwords for the school network and any other online facility must be kept secret and must be changed regularly. Inform IT Services if you believe someone has obtained your passwords. Use passwords that are difficult to guess, and do not let anyone see you entering your passwords. It is good practice to have different passwords for different systems rather than the same password for all. Do not log on to a computing device or any ICT system using another person's password, or use such devices or systems that have been left logged on prior to your use. When you have finished a session, exit and close any IT systems and always log off computers and any password protected sites.

11. Network Folders

School network folders, including VLE content and folders, are school property and should therefore be used for the storage of school-related work only. Student network and VLE folders may be scanned from time to time, and the school reserves the right to remove or delete any non-educational content without notice.

12. Monitoring

Millfield School has the right to monitor the ICT activity of students to ensure safe and proper use of its IT systems and to protect its members (staff and pupils).

13. Software

Software is not to be installed on any of the ICT facilities. Downloading or the installation of executable files (.exe) is forbidden.

14. Backing-up work

Files stored on the school network drives are regularly backed up by IT Services for the purpose of disaster recovery. These backups are only maintained for 30 days. It is your responsibility to back up important work, by regularly transferring copies home, or storing electronic copies of work in a safe place. If you have lost work on school IT systems, please contact IT Services to attempt recovery of files. You are responsible for the safe storage and backing up of work held on online services and websites. Always keep a copy of material stored in Cloud-based services, as these provide no guarantee of safety or security. When using mobile devices important work should be saved to the school network via the FOLDR facility.

15. Copyright

You must not copy or store files, documents, music, video, or any other material where copyright restrictions exist, unless permission by the copyright holder has been given. Any external work that is used by you in your studies & in coursework should be clearly referenced and acknowledged in accordance with examination board guidelines. Using copyright material without permission is an offence under the Designs Copyrights and Patents Act.

16. Prevention of viruses

It is recommended that you have suitable anti-virus protection at home and on any personal computing/mobile devices that you use. In addition, all devices and software should be kept up to date. For Windows based devices accessing the school network anti-virus software is a requirement due to the higher level of risk. Where IT Services are concerned in relation to the risk presented by any device attempting to access the network such devices may be prevented from access. Do not open attachments to e-mails or click on links if you are suspicious or uncertain who the sender is. Do not introduce to the school network any removable device (e.g. USB memory stick) that you suspect is infected. If you suspect a virus is present on any school system, please contact IT Services.

17. Protecting the school network

You must not attempt to gain administrative access to the School's network or bypass security restrictions. If you discover a problem with the School's network security, do not demonstrate the problem to other users. Instead, you should report it immediately to IT Services. The Computer Misuse Act 1990 makes it a criminal offence to gain unauthorised access to a computer system in order to view or change information. The School reserves the right to inspect data files and network logs in order to investigate complaints.

18. Liability

Users' work areas are scanned daily for the presence of viruses, and files are automatically disinfected, but the School accepts no liability for any damage caused by computer viruses, however they originate. The School accepts no liability in the unlikely event that damage is sustained to your computer/tablet/mobile device as a result of its being connected to our network. Although our systems offer a very high level of protection, the School can ultimately accept no liability for data loss or its consequences.

19. Printing

You can print from most networked computer locations in school, but charges may apply. Please do not tamper with, maintain, or install cartridges in printing devices. Please report any faults or problems to a supervising teacher or IT Services.

20. Use of ICT rooms and equipment

ICT rooms and equipment must be left in good order; any damage must be reported to your supervising teacher or to IT Services.

21. Breach notification

Where users suspect or are aware that unauthorised access to their computer or a school account has occurred they must report this to IT Services immediately so that appropriate action can be taken.

Declaration

By using personal, online, and school-provided ICT facilities and systems at Millfield School I agree to comply with the rules described in this document and:

1. I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour through my use of ICT, in school and when I am out of school and where such incidents involve my membership of the school community.

2. I understand that if I fail to comply with this agreement, I may be subject to disciplinary action. This may include: loss of access to facilities, removal of personally owned tablet/mobile/web enabled devices, detentions, suspensions, and contact with parents and in the event of illegal activities, the involvement of the police.

3. I understand that this agreement covers my use of school ICT systems and equipment, and my use of my own equipment in school when allowed (e.g. laptops, tablets, mobile phones, PDA's, cameras etc.). This agreement also covers my use of my own equipment out of school and my use of online facilities when its use impacts on me being a member of the school community.

4. The specifics of this document are subject to change as technology evolves, and I understand that the intent of this document will still apply, and further guidance from time to time will be communicated to me.

Version Control		
Version	Date	Details
	20/09/2017	Reviewed and updated by JMF/SCL.
	12/04/2018	Addition of Updates and AV requirement changes to section 16.
1.8	14/05/2018	Modified to incorporate items from the ISBA Sample Accepted, SMT (Senior School)
1.8	22/06/2018	Accepted, SMT (Prep School)