Summary of key policy guidelines:

- This policy applies to **all computers and devices** including **personal mobile and tablet devices** that you use in school, and also to your **online behaviour** towards Millfield and other users inside and outside of school.
- **Do not record sound, video, take photographs** on any device unless you have appropriate permission and consent to do so. Do not upload online, share or broadcast any such content unless you have permission and consent to do so. Please consult the schools Social Media Policy for further guidance.
- **Do not upload or share images, video and other content** that is indecent or could embarrass or harass others, or could break the law.
- Protect your identity online by **not sharing passwords, not uploading personal details** of you or other users. Regularly check and review your privacy settings on online sites & accounts.
- Electronic contact & discussions **must be respectful and appropriate at all times**. Electronic communication should be treated with the same care as a letter on school headed paper.
- Do not publish or share any information that defames, undermines, misrepresents, or tarnishes the reputation of others, the school or its users.
- Report any suspicious online inappropriate or threatening behaviour to **IT services or the schools DSL where necessary.**
- Always ensure that mobile and tablet devices have **passcodes, passwords, biometrics, etc. switched on**, and that passcodes or passwords are not revealed or shared with others.
- Do not access unsuitable or inappropriate material online.
- Always make use of strong passwords for school systems and also for other online services. Further guidance on creating strong passwords is available from IT Services.
- **Accessing someone else's computer, phone or tablet or school/online accounts** without that person's permission is illegal.
- **The school may monitor your use of IT systems and online behaviour** to maintain safety and also compliance with this policy.
- Do not install software onto the school network, or try to circumnavigate any of the network and ICT controls that are in place.
- Always ensure that personal data is secure and that you comply with the schools Data Protection Policy.
- **Copying files** (images, music, video, text) that are copyright protected is against the law.
- ICT use can pose a health risk; always ensure your seating position is appropriate to prevent strain and that you take regular breaks from screen use.
- Further advice can be sought from IT Services

A full copy of the policy is available on request or from the schools Xtranet

1. Use of Mobile Learning technologies and school WIFI

The content of this policy applies to all IT devices connected to the school network, school systems and other devices or online services used in conjunction with school activities including but not limited to personal devices, school issued devices, desktop computers, etc. Within this policy the School and Millfield are used to refer to the Senior School and Prep School sites including EYFS provision, Enterprises, OM Society and Development Operations. Separate guidelines are provided on school issued iPads as issued to teachers and some other students/staff. The school reserves the right to monitor, remove, reconfigure, and suspend use of devices connected to the network and content to ensure compliance with this policy. The recording of sound, images or video should only be undertaken where permission and consent has been established. Do not upload online, share or broadcast any such content unless permission and consent has been established. 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.

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. Where possible avoid using your own photographs to identify yourself online, try to use an avatar or cartoon images instead. Where photographs are required these should be professional and appropriate to their usage.

3. Protecting yourself from Internet dangers

Report any suspicious or inappropriate approaches, messages or similar online behaviour to IT Services and the schools DSL where necessary. 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 others must be respectful and appropriate at all times. Electronic contact with pupils must be only as part of approved school activities and should only be made from school user accounts.

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 appropriate permission and consent exists. 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. Further guidance is available in the schools Social Media policy.

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'.

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 or where using Millfield systems/services, and therefore the guidelines described within this document apply when such devices are being used.

All personal devices should have adequate security to ensure data is not accessible by people other than Millfield staff authorised to access the data, including using user account login details and data encryption.

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 or via any school IT system or try to bypass school filtering or password security controls. Access to unsuitable content includes but is not limited to: 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 4G/5G, 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. You must use strong passwords for the school network and any other online facility and these passwords must be kept secret. 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. You should 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 content and folders in OneDrive, Teams and Sharepoint, are school property and should therefore be used for the storage of school-related work. Network folders may be scanned from time to time, and the school reserves the right to remove or delete inappropriate content without notice.

12. Monitoring

Millfield School has the right to monitor the ICT activity of users on school devices or where personal devices make use of school systems, 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

The school makes every effort to protect school data from loss. Users should therefore ensure data is stored on school storage solutions including on network storage, OneDrive, Teams and Sharepoint.

Users are responsible for ensuring that data they require is not accidentally deleted and for the safe storage and backing up of work held on online services, websites and mobile devices. When using mobile devices important work should be saved to OneDrive.

15. Data Protection

Users must comply with the Data Protection Act 2018, GDPR and the schools Data Protection Policy and Guidelines, as well as any other legislation which applies at the time. Where any doubt exists you should contact the schools Information Privacy Officer.

16. 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.

17. 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.

18. 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.

19. 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.

20. Printing

You can print from most networked computer locations in school. Please consider carefully before printing. In addition charges may apply. Please report any faults or problems to IT Services.

21. Use of ICT rooms and equipment

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

22. Health and Safety

Use of ICT equipment can pose health risks. It is your responsibility to seek clarification and advice on this issue from the Schools' nominated Health & Safety representative and understand school Health & Safety policies.

In general terms, staff should avoid eye-strain by taking regular breaks from viewing the screen, adjust keyboards, screens, and desk positions to prevent strain and promote good posture. Users should ensure that adjustable chairs are adjusted to the correct position applicable to themselves.

23. Disposal of equipment

All IT equipment reaching end of life or where it is no longer used must be disposed of safely and securely. Where devices, particularly those with data storage capacity, are no longer being used they should be passed to IT services for secure display via an authorised disposal company.

24. 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.

25. Where to obtain advice

Advice can be sought from your line manager or IT Services.

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.

2. I understand that if I fail to comply with this agreement, I may be subject to disciplinary action. This may include: restricted or loss of access to facilities, disciplinary action, dismissal/expulsion and 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, PDAs, cameras etc.). This agreement also covers my use of my own equipment out of school where accessing school systems and my use of online facilities when its use impacts on the school as a result of 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
	Sept 2015	SCL/JMF Staff IT AUP
	Feb 2017	Revised to align with Pupil AUP
	11/10/2017	Minor amendment to para 1. to include devices and services used in conjunction with school activities.
	16/10/2017	Accepted, SMT (Senior School)
	31/10/2017	Added a scope statement and direct reference to EYFS.
	17/11/2017	Changes made in response to Prep SMT review.
	12/04/2018	Addition of Updates and AV requirement changes to section 17.
	01/05/2018	Updated with reference to OS updates.
	05/05/2018	Modified to incorporate items from the ISBA sample AUP.
1.5	14/05/2018	Accepted, SMT (Senior School)
1.5	22/06/2018	Accepted, SMT (Prep School)
1.6	15/07/2019	Updated, G.Henderson
1.7	04/08/2020	Update, G.Henderson; replace mention of staff with Users.
1.8	24/05/2021	Update, G.Henderson; Pt4: Refers to “supervising member of staff” rather than “line manager”