Yehudi
Menuhin
School

E-Safety Policy Group

Incorporating:

Staff E-Safety Policy: Keeping pupils safe online,
Acceptable Use of IT Policy for Staff,
E-Safety Guidance & IT Acceptable Use Policy for Pupils,
Bring your own device (BYOD) Policy for Staff & Visitors
AI Policy for Staff

CONTENTS

Summary of material changes since the previous version

Revision	Revision
November 2017	
December 2020	Updated Format.
February 2023	Updated Format. Replaces previous policy 8.1. Policy updated to reflect latest developments in technology, use of devices, remote learning and KCSIE. Updated agreement form for pupils.
September 2023	Updated to include new KCSiE references to appropriate filtering and monitoring systems
June 2025	Introduction of new BYOD Policy Introduction of new AI Policy Updates to Acceptable use policies (staff & pupils) with AI guidance and updates to Letter to Parents Removal of Image Consent Form (now part of new standalone Taking, Storing and Using Images of Children Policy)

Abbreviations, Acronyms and Definitions

Abbreviation / Acronym	Definition
Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Roaming	When you are traveling abroad, data roaming will take over from your mobile data. It allows you to access the internet in other countries. Keep in mind that data roaming will cost you extra.
Data Subject	The identified or identifiable living individual to whom personal data relates.
DSL	Designated Safeguarding Lead
INSET	In Service Education and Training
Leadership Team	Consists of: Headmaster, Deputy Head (Academic), Deputy Head (Pastoral), Director of Music, Bursar, Director of Development

Microsoft 365	A product family of Microsoft software including Office apps, cloud services and security solutions.
Microsoft Office Suite	: the family of Microsoft products that includes: Microsoft Word (written documents) Microsoft PowerPoint (presentations) Microsoft Excel (spreadsheets) Microsoft Outlook (emails, contacts & calendars) Microsoft OneNote (digital notebook) Microsoft OneDrive (cloud-based drives for saving files) Microsoft Teams (communication hub for messaging, document sharing, group working, video calling)
Mobile Data (Cellular Data)	Mobile data is internet content delivered to mobile devices such as smartphones and tablets over a wireless **cellular** connection.
Network/Mobile Network ***also known as a cellular network***	The wireless communication system that enables devices like phones and tablets to connect and exchange information. The mobile network infrastructure in the UK is owned by four mobile operators: O2, EE, Vodafone and Three. Any other mobile network will pay one of these companies to use the infrastructure and therefore the service will be cheaper but not necessarily as good. In the school's local area, we find O2 or Three seems to work best.
Parents	Adults with parental authority for a child
Personal Data	Any information relating to a person (a 'data subject') who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
Personal Device	Any piece of electronic equipment not provided by the school, purchased by an individual for their personal use including (but not limited to) mobile phones, tablets, laptops and desktop computers.
Plagiarism	The act of taking someone else's work and passing it off as one's own.
PSHE	Personal, Social, and Health Education
School data	Data held by and/or belonging to the school including but not limited to personal data held about pupils, staff and visitors.

School IT Resources & Communication Systems	Any IT service provided by the school to its staff and pupils for school operations, including (but not limited to) Microsoft 365 accounts (Microsoft Outlook (school email), Microsoft Teams, OneDrive, SharePoint etc.), Windows Computer access and all school Wi-Fi networks.
Wi-Fi (Wireless Fidelity)	Internet access without wires/cables.

Difference between Wi-Fi & Mobile Data: Wi-Fi is limited to being within range of a Wireless router / Access Point (AP) whilst Mobile data is limited only by your phone signal and therefore your phone network provider's coverage. Data transmitted over Wireless is limited by the quality of the router and your phone. Mobile data can be controlled with data caps through your phone plan.

Part A: Staff E-Safety Policy: Keeping Pupils Safe Online

1. AIM / OBJECTIVE / STATEMENT OF INTENT

Introduction

This document consists of:

- The E-Safety Policy for Staff
- The Acceptable Use of IT Policy for Staff
- The Acceptable Use of IT Policy for Pupils and Guidance for Pupils on E-Safety
- Appendix A: The Letter to Parents about Technology
- Appendix B: The Image Consent Form

It is the duty of The Yehudi Menuhin School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

The School recognises, as part of its constant striving to provide safe online activity for its pupils, its duty to meet the DfE's Filtering and Monitoring Standards, Cyber Security Standards and Guidance on keeping children safe in out-of-school settings. The latter makes it clear that the School's duty of care, including our responsibility to keep our pupils safe online, does not end at the school gates, but continues whenever and wherever we are looking after them.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

This policy is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding and Child Protection Policy
- Staff Behaviour Policy
- Staff Code of Conduct
- Behaviour Management Policy
- Anti-Bullying, Racial or Sexual Harassment Policy
- Privacy Notice for Parents & Pupils
- Privacy Notice for Supporters
- Privacy Notice for Job Applicants & Staff
- Data Retention Policy
- Personal, Social and Health Education (PSHE) Policy

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At The Yehudi Menuhin School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the IT Acceptable Use Policy (for all staff, visitors and pupils) cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

2. ROLES AND RESPONSIBILITIES

The Head and the Senior Leadership Team

a) The Head is responsible for the safety of the members of the school community and this includes responsibility for e-safety.
b) The Head has delegated day-to-day responsibility to the Deputy Head (Pastoral)/DSL (in the capacity of e-safety coordinator) and the Bursar (as data protection lead).

c) In particular, the role of the Head and the Senior Leadership team is to ensure that:
   i. staff, in particular the e-safety coordinator, are adequately trained about e-safety; and
   ii. staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

DSL (in the role of E-safety coordinator)
The School's DSL is the e-safety coordinator and is responsible to the Head for day-to-day issues relating to e-safety. The e-safety coordinator has responsibility for ensuring this policy is upheld by all members of the school community and works with IT staff to achieve this. They will keep up-to-date on current e-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board. They will ensure school policies relating to e-safety follow all statutory regulations and guidance, such as KCSiE and ISSR/NMS.

As part of this role, the DSL is responsible for overseeing the filtering and monitoring of the School's IT network. They regularly review the effectiveness of the School's online filtering systems with IT staff and receives automatic notifications of any attempts by pupils or staff to view unacceptable material online using the School's network.

Bursar
The **Bursar** is responsible for the School's technical provision and infrastructure, working with the School's IT providers to ensure that safeguards are in place to filter and monitor inappropriate content and alert the School to safeguarding issues. The school's IT staff have a key role in maintaining a safe technical infrastructure at the school. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT.

The Bursar delegates the day-to-day oversight of the infrastructure and communication with the IT support providers to the Head of IT.

The Head of IT has a key role at the school. They are the key communicator between the school and the school's appointed **IT Support provider**; EducAite who are responsible for the security of the school's hardware system, its data, maintaining a safe technical infrastructure and in keeping abreast with the rapid succession of technical developments. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the e-safety coordinator.

The Head of IT is responsible for training the school's teaching staff in the use of IT.
Deputy Head (Academic)
The Deputy Head (Academic) is responsible for ensuring that the curriculum includes education and guidance for pupils on the safe use of technology and the provision and restrictions that apply to the use of technology in School. This part of the curriculum is delivered in PSHE lessons. The Head of PSHE liaises with the Deputy Head (Academic) and the E-safety Coordinator to ensure the PSHE curriculum follows all statutory regulations and guidance.

Governors

Governors have a responsibility to challenge the DSL, and LT in general, on their oversight of the School's online filtering and monitoring systems.

House staff

The House staff will ensure that younger pupils have limited access to their mobile devices (and thus 3G, 4G and 5G provision).

Expectations of Teaching and Support Staff

- All staff are required to sign the IT Acceptable Use Policy before accessing the school's systems.
- As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis. The forum for this would be at fortnightly Pastoral meetings. In addition, the school has an annual IT review, and staff are encouraged to submit larger concerns or recommendations to the committee ahead of its yearly meeting.

Pupils

Pupils are responsible for using the school IT systems in accordance with the IT Acceptable Use Policy, and for letting staff know if they see IT systems being misused.

All pupils:

- are responsible for using school digital technology systems in accordance with the school acceptable use policy;
- will understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
- will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- are expected to understand policies on the use of mobile devices and digital cameras, the taking / using of images and cyber-bullying; and
- will understand that the e-safety policy will include actions outside of school where related to school activities.

Parents / Carers

The School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school and reports annually to parents about use of technology. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school. Parents and carers are responsible for endorsing the school's IT Acceptable Use Policy where it applies to pupils.

Community Users / Contractors

Where such groups have access to school networks / devices, they will be expected to provide signed acceptance to abide by school e-safety policies and procedures. Guest users have their access to the internet restricted by the School.

3. EDUCATION AND TRAINING

Staff: awareness and training

New staff receive information on The Yehudi Menuhin School's e-Safety and IT Acceptable Use policies from the E-Safety Coordinator as part of their induction.

All staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All supply staff and contractors receive information about e-safety as part of the Safeguarding information they are given on arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. These behaviours are summarised in the IT Acceptable Use Policy which must be signed and returned before use of technologies in school. When children access the school network (via school computers, the school wi-fi network or their Microsoft accounts), staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A CPOMS report must be completed by staff as soon as possible if any incident relating to e-safety occurs. This report will be addressed by the school's e-safety Coordinator/DSL.

Pupils: e-safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in Morning Meetings, as well as informally when opportunities arise.

At age-appropriate levels, and usually via PSHE, pupils are taught about their e-safety responsibilities and to look after their own online safety. From C2, pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Deputy Head (Pastoral)/DSL (the e-Safety Coordinator) and any member of staff at the school.

Pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

Pupils are made aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the DSL, School Counsellor, Heads of Section, Boarding staff as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Pupils are also taught about the effects of online peer pressure and bullying with a focus on how to report should they encounter it.

Parents
The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore provides an updated letter for parents each year with guidance surrounding devices and encourages parents to contact the DSL/E-Safety Co-ordinator for support.

4. USE OF SCHOOL AND PERSONAL DEVICES

Staff
School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for schoolwork. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. [Devices issued to staff are encrypted, to protect data stored on them].

Staff at The Yehudi Menuhin School are permitted to bring in personal devices for their own use, providing they abide by statutory regulations and follow School policies on E-Safety and Data Protection.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents / carers and under no circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system with the exception of Microsoft Teams on their school-provided account.

Pupils
Pupils are required to bring a mobile device to school with them, for the purpose of communicating with house staff and teachers via their school-provided Microsoft accounts. Boarding pupils in C1, C2 and C3 are required to hand in all devices that communicate over the internet, including smartwatches and other wearable technology, to Boarding staff 30-minutes prior to lights out each evening. Devices will be stored securely and can be collected the following morning after alarms have been deactivated.

School devices for pupil use [laptops/tablets] are available for short or long-term loan, at the request of pupils/pupil parents with written support of a member of the Head of IT. The parents of pupils who qualify for the Electronic Device loan scheme will be required to sign the Electronic Loan Agreement for the specific device being loaned.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the Head of IT to agree how the school can appropriately support such use. The Head of IT will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

5. USE OF INTERNET AND EMAIL

Staff

Staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must immediately report to DSL/e-Safety Coordinator the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to ITSupport@menuhinschool.co.uk.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm
- bring The Yehudi Menuhin School into disrepute
- breach confidentiality
- breach copyright
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
  - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age
  - using social media to bully another individual
  - posting links to or endorsing material which is discriminatory or offensive

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email/WhatsApp address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. The Staff Code of Conduct sets out clear expectations for staff communication with pupils.

6. USE OF VPNs (Virtual Private Networks)

VPN or Virtual Private Networks create a private connection between a user's device and a remote server which then connects to the Wi-Fi network on your behalf. Remote servers can be based in another country, allowing you to appear as if you are in that country when browsing the internet, however it stops a network from being able to identify your device. This is very helpful when connected to public networks (such as trains, cafes, airports) however is not appropriate in a school environment where our role is to monitor and protect our pupils.

Pupils are not permitted to use VPNs to bypass school content filters or access restricted websites. If staff become aware of a pupil using a VPN they should report this to Head of IT. This may result in sanctions in line with the school's Rewards and Sanctions policy.

Pupils who experience issues accessing appropriate apps / websites should be encouraged to report this to the Head of IT to have them unblocked through the school's systems. This will in turn improve the Wi-Fi experience for other pupils.

7. SOCIAL MEDIA

The School recognises the unique nature of being a specialist music school educating young musicians already in the process of developing a career in music and potentially promoting themselves publicly and online. Many staff of The Yehudi Menuhin School are active musicians, with thriving musical careers reliant on modern promotional platforms, however under no circumstances should staff contact school pupils or parents via accounts not provided by The Yehudi Menuhin School.

Under no circumstances should school pupils or parents be added as social network 'friends' or contacted through social media. The Yehudi Menuhin School seeks to support the professional development of its staff and acknowledges the important role social media can now have in professional performing careers. Staff with professional social media accounts visible to the public should be aware of the likelihood of pupils finding and potentially following them. Pupils may choose to follow staff on professional social media profiles and reminds staff to remain aware of this likelihood when sharing/posting to their social media. It is important staff keep in mind that even if a pupil does not follow their professional accounts, public accounts are still searchable and visible.

Pupils

All pupils are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure and must be used for all schoolwork (assignments / research / projects). Pupils should be aware that email communications through the school network and school email addresses are monitored.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for schoolwork / research purposes, pupils should contact a member of staff for assistance who will raise the issue with the Head of IT for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to the DSL/e-Safety Coordinator or a member of boarding/pastoral staff.

The school expects pupils to think carefully before they post any information online or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the e-Safety Coordinator. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded and will be dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for schoolwork / research purposes, pupils should contact a member of staff for assistance.

Data storage and processing

The school takes its compliance with the Data Protection Act 1998 seriously. Please refer to the appropriate Privacy Notices (Parents & Pupils / Supporters / Job Applicants & Staff) and IT Acceptable Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to their Microsoft OneDrive Account, accessible via their school-provided email account. Any files incompatible with OneDrive can be stored on school network drives.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead staff or pupils should request an encrypted USB memory stick which, if authorised, will be provided by the School.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the DSL/e-Safety Coordinator.

8. PASSWORD SECURITY

Pupils and staff have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password for every account they have access to (12-16 characters)
- follow best practise guidance for creating a password which can be found in the school's IT Acceptable Use Policy
- change their password when prompted (every 42 days for AD accounts)
- not write passwords down; and
- not share passwords with other pupils or staff.
- Change their password immediately if they suspect it has been compromised and log out all current logins on all devices.
- Use a password manager/vault

9. SAFE USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Parents / carers should refer to the P94 Taking, Storing and Using Images of Children policy, Section 7: Use of cameras and filming equipment (including mobile phones) by parents which detail when photography/videography is and is not acceptable at school events.

All programmes for events at the Menuhin Hall include a line reminding the audience that it is prohibited to take photographs and videos and this includes parents, guardians or close family members.

Staff and volunteers are allowed to take digital / video images on behalf of the school but must follow the Taking, Storing and Using Images of Children Policy & the Bring Your Own Device (BYOD) Policy. **Images should only be taken on school devices: personal devices should not be used for such purposes**.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils are made aware that to take, use, share, publish or distribute images of others without express permission from the individual/s may be a breach of Data Protection laws. Pupils should find further guidance in P94 Taking, Storing and Using Images of Children policy, Section 8: Use of cameras and filming equipment by pupils.

For further information about the consent for and use of images by the school can be found in the Taking, Storing and Using Images of Children policy.

10. MISUSE

The Yehudi Menuhin School will not tolerate illegal activities or activities that are inappropriate in a school context and will report illegal activity to the police and/or the Local Safeguarding Children Board. If the school discovers that a child or young person is at risk because of online activity, it may seek assistance from the CEOP.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures (in particular the Safeguarding Policy).

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

11. COMPLAINTS

As with all issues of safety at The Yehudi Menuhin School if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the DSL/e-Safety Coordinator in the first instance, who will liaise with the leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of or concerns around e-safety will be recorded on CPOMS and reported to the school's DSL/e-Safety Co-ordinator, in accordance with the school's Safeguarding and Child Protection Policy.

12. REPORTING

If concerns about e-safety arise which involve Child Protection issues they should be reported to the DSL immediately.

Other e-safety issues should be reported to the Head, who will involve the Leadership Team, as necessary, to manage the issues.

If pupils raise issues concerning e-safety to pastoral or other staff, this should be raised to the DLS/e-safety co-ordinator as soon as possible.

Part B: IT Acceptable Use Policy (Staff)

1. INTRODUCTION

This policy applies to all staff who use school IT systems, as a condition of access.

2. ONLINE BEHAVIOUR

As a member of the school community, you should follow these principles in all of your online activities:

- The school cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

3. USING THE SCHOOL'S IT SYSTEMS

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.

- Do not attempt to install software on, or otherwise alter, school IT systems. If you require access to specific software to aid in lessons, this can be requested via the Head of IT who will seek approval from the school's designated approvers.

- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.

- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

4. PASSWORDS

Passwords protect the School's network and computer system and are your responsibility. They should not be the same as your widely used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Staff are advised/required to follow best practise for password generation:

- *When creating passwords, think hard to guess, easy to remember! The longer the password the better (12-16 characters is optimum)*
- *Avoid easy to guess passwords such as family members names, pet's names or birthdays, or a repeated/series of characters such as 12345 or AAAAA or qwerty.*
- *Avoid single words followed by a single number.*
- *Avoid words that can be found in a dictionary, in any language. One way to do this is to try to combine two unrelated words.*
- *Complexity helps – try to use a mix of upper- and lower-case letters, numbers and special characters (such as !?&,@"#).*
- *If you struggle to remember all your passwords, use a password manager/password vault such as LastPass or LogMeOnce.*
- *Passwords should be changed every 3-6 months.*
- *If you suspect your password has been compromised, change it immediately and if given the option log yourself out of all current logins on all devices.*
- *A good approach to password is to think of a phrase you will remember then shortening it, substituting letters with numbers and special characters and mix the case, such as:*
  Vibrato to finish = v1br@to2Fnsh
  From Saddle to Scroll = FrmS4ddl32Scr0!!
  Knight takes Bishop = Kn!ghtT@k3B1sh0p

Staff AD (Active Directory) account passwords (which allow access to school devices) are required to be changed every 42 days.

Microsoft account passwords do not expire; however, staff are required to use 2FA/MFA (two/multi-factor authentication) on accounts wherever possible, particularly but not limited to Microsoft 365 accounts (Outlook, Teams etc.), CPOMS, iSams and any other account which has access to sensitive/confidential information. You should never attempt to gain unauthorised access to anyone else's accounts or to confidential information to which you do not have access rights.

5. USE OF PROPERTY

Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the Bursary department, via the Head of IT.

6. USE OF SCHOOL SYSTEMS

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

7. USE OF PERSONAL DEVICES OR ACCOUNTS AND WORKING REMOTELY

All official school business of staff and governors must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the Bursary department, who oversee our Data Protection.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies, as detailed on in the Data Protection Policy and BYOD device policy

For the purpose of IT designation, staff are allocated to one of three groups; Administrative Staff, Academic Teaching staff and non-academic Teaching staff. Administrative staff includes all members of LT.

All **administrative staff** will be provided with access to a computer device as appropriate for their role, and reflecting the nature of work they are required to undertake. Where possible the school will support the option for remote working in keeping with the school's Flexible Working Policy (P4.6).

All **academic teaching staff** (unless self-employed) will be provided with a portable device compatible with teaching classroom set-ups.

All **non-academic teaching staff** will not be allocated a school device, under the assumption this is not required for their role. Exceptions will be made at the request of line managers, on a temporary or permanent basis. Non-Academic teaching staff are encouraged to speak to their line manager if they feel a school device would aid in their teaching.

Some staff may also be provided with a mobile telephone device if deemed appropriate for their role.

All staff are provided with a Microsoft 365 account which provides them with access to a Microsoft Outlook email inbox & Microsoft Teams account for communication within the Yehudi Menuhin School community, access to a OneDrive and SharePoint for secure file storage.

8. USE OF AI (ARTIFICIAL INTELLIGENCE)

Staff are permitted to use AI tools where appropriate to support their role within the school. AI should only be used to assistant staff to work more efficiently and effectively and not rely on AI to complete work without human involvement. When using AI tools, staff must:

- only input anonymized data into AI systems to avoid the exposure of personally identifiable or sensitive information
- always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school
- only use AI technologies approved by the school along with school-provided AI accounts for work purposes
- not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognize and safeguard sensitive data
- be mindful of copyright infringement and the potential for the misuse of intellectual property, including the intellectual property pupils hold over their schoolwork. Care must be taken to avoid intellectual property being used to train generative AI models without appropriate consent
- be mindful of the risk of discrimination and bias in the outputs from AI tools. Staff should be critical in evaluating AI outputs for bias and discrimination and always follow due care and diligence to prioritise fairness and safety particularly when it comes to assessing pupils' work
- be aware that any and all AI generated content should be reviewed for factual consistency
- be aware that they are responsible for any incorrect information presented that has been provided or assisted by AI-generation
- be transparent about when they are using AI-Generated content, both inside and outside the classroom with both staff, pupils and external parties. Any documents, emails presentation and other outputs generated or influenced by AI should be presented with clear labels or notes indicating AI assistance

- report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the Data Protection Lead and the Head of IT in line with any other cyber security concerns
  In the first instance this can be an email, however staff must be prepared to provide further information should an investigation be deemed necessary

For further guidance and information about the school's AI usage, please refer to our AI Policy (E-Safety Policy Group Part E).

9. MONITORING AND ACCESS

Staff should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

As stated in the parent contract, any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined under such circumstances. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

10. RETENTION OF DIGITAL DATA

Staff must be aware that all staff Microsoft 365 accounts including Microsoft Outlook email inboxes and school computer (AD) accounts will be disabled upon departure from the school. Deletion of accounts will vary dependent upon the role as some access may need to be retained by a successor to a role but cannot be guaranteed.

Any information from email folders that is necessary for the school to keep for longer, including personal information (e.g. for a reason set out in the school privacy notice), should be held on the relevant personnel or pupil file.

Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

If you consider that reasons exist for the protocol not to apply or need assistance in how to retain and appropriately archive data, please contact the Bursary.

11. BREACH REPORTING

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, e.g., through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email;
- unsecure disposal; and
- Inappropriate input into AI systems.

The school must generally report personal data breaches to the ICO without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff become aware of a suspected breach, they should notify the Data Protection Lead as soon as possible and confirm receipt of notification by phone. If the Data Protection Lead is not available, the IT Co-ordinator and e-Safety Co-ordinator should be notified immediately. Staff should document and share with the Data Protection Lead details of the breach: how long, what data & how far has the data got?

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

12. BREACHES OF THIS POLICY

A deliberate breach of this policy by staff will be dealt with as a disciplinary matter using the school's usual applicable procedures. In addition, a deliberate breach by any person may result in the school restricting that person’s access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the **Designated Safeguarding Lead** (in the case of concerns regarding online harassment or harm) or the **Bursar** (for any other concerns). Reports will be treated in confidence wherever possible.

ACCEPTANCE OF THIS POLICY

Please confirm that you understand and accept this policy by signing below and returning the signed copy to Gemma Lawrence, HR Administrator (Staff/Governors).

I understand and accept this acceptable use policy for staff:

Signature: ___________________________________

Date: ________________________

Name: ______________________________________

Part C: E-Safety Guidance and IT Acceptable Use Policy (Pupils)

1. INTRODUCTION

Scope of this Policy
This policy applies to all pupils of the school who use school IT systems, as a condition of access.

2. ONLINE BEHAVIOUR

As a member of the school community, you should follow these principles in all your online activities:

- The school cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Pupils should not attempt to discover or contact the personal email addresses or social media accounts of staff.

3. USING THE SCHOOL'S IT SYSTEMS

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.

- Do not attempt to install software on, or otherwise alter, school IT systems. If you require access to specific software to aid in lessons, this can be requested via the Head of IT who will seek approval from the school's designated approvers.

- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.

- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

4. PASSWORDS

Passwords protect the School's network and computer system and are your responsibility. They should not be the same as your widely used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Pupils are advised/required to follow best practice for password generation:

- *When creating passwords, think hard to guess, easy to remember! The longer the password the better (12-16 characters is optimum)*

- *Avoid easy to guess passwords such as family members names, pet's names or birthdays, or a repeated/series of characters such as 12345 or AAAAA or qwerty.*

- *Avoid single words followed by a single number.*

- *Avoid words that can be found in a dictionary, in any language. One way to do this is to try to combine two unrelated words.*

- *Complexity helps – try to use a mix of upper- and lower-case letters, numbers and special characters (such as !?&,@"#).*

- *If you struggle to remember all your passwords, use a password manager/password vault such as LastPass or LogMeOnce.*

- *Passwords should be changed every 3-6 months.*

- *If you suspect your password has been compromised, change it immediately and if given the option log yourself out of all current logins on all devices.*

- *A good approach to password is to think of a phrase you will remember then shortening it, substituting letters with numbers and special characters and mix the case, such as:*
Vibrato to finish = v1br@to2Fnsh
From Saddle to Scroll = FrmS4ddl32Scr0!!
Knight takes Bishop = Kn!ghtT@k3B1sh0p

Pupil AD (Active Directory) account passwords (which allow access to school devices) are required to be changed every 42 days.

Pupil Microsoft account passwords do not expire. You should never attempt to gain unauthorised access to anyone else's accounts or to confidential information to which you do not have access rights.

5. USE OF PROPERTY

Any property belonging to the School should be treated with respect and care and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the Bursary department, via the Head of IT.

6. USE OF SCHOOL SYSTEMS

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

7. USE OF PERSONAL DEVICES OR ACCOUNTS AND WORKING REMOTELY

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies, as detailed on in the Data Protection Policy.
Pupils are permitted to bring to site a personal mobile telephone device in addition to a laptop computer/tablet to aid in their studies. Details and guidance regarding pupil devices can be found in Appendix A: Letter to Parents.

8. USE OF AI (ARTIFICIAL INTELLIGENCE)

The school recognises the growing use of AI (Artificial Intelligence) and aims to equip pupils with the knowledge and skills to use AI in an ethical and responsible way that will benefit them in a changing technological landscape. However pupils must also be aware that there are both ethical and safety risks associated with use of AI.

Pupils' use of AI should come from a place of intellectual curiosity and creativity with a goal of supporting their own learning. They should engage in open dialogue with teachers about how AI can support their learning and aim to understand why certain usage is discouraged/restricted.

Pupils must:

- **Not input sensitive data/information about themselves or others into any AI tools**
  Sensitive data/information includes but is not limited to names, dates of birth, addresses as well as images, audio recordings or video recordings of themselves or others. Due to the nature of AI's ability to learn from the data input in to it, pupils must be wary of providing AI tools with access to data about themselves and others.

- **recognise that excessive/inappropriate use of AI in their school work could be detrimental to their learning**
  Pupils should recognise that getting AI tools to complete work for them only results in damage to their own learning by not allowing teachers to check their understanding of topics covered or allowing them to test and demonstrate their own learning.
- **Be transparent with teachers where and when they are using AI to support their academic work.**
  This can include using AI to generate essay templates, using AI to summarise class notes or explain assignments to support understanding of set work. This also includes the use of AI translation tools to aid non-native English speakers to understand assignments, however transparency is key so that teachers can help to mitigate issues with translation errors.
  Likewise, teachers and staff should be transparent with pupils about their use of AI to generate classroom materials.
- **Not use AI to complete coursework or other exam materials.**
  Pupils should follow all teacher instructions on the use of AI when concerning their exam subjects to ensure they are not committing plagiarism. The school cannot shield pupils who are caught using AI in their exam subjects.
- **Recognise that AI chatbots are designed to seem friendly and approachable, however are no replacement for real human interaction and advice.**
  Pupils should always keep in the forefront of their minds that AI interfaces are a system of complex algorithms designed to predict the most likely answers to their queries. They do not have feelings, emotions and can only simulate true empathy. If a pupil is concerned or in need of support, they should reach out to real people.
- **Only use school-approved AI tools to support them with school life.**

9. USE OF VPNs (Virtual Private Networks)

VPN or Virtual Private Networks create a private connection between a users device and a remote server which then connects to the Wi-Fi network on your behalf. Remote servers can be based in another country, allowing you to appear as if you are in that country when browsing the internet, however it stops a network from being able to identify your device. This is very helpful when connected to public networks (such as trains, cafes, airports) however is not appropriate in a school environment where our role is to monitor and protect our pupils.

Students are not permitted to use VPNs to bypass school content filters or access restricted websites. Pupils found using VPNs will likely receive sanctions in line with the Rewards and Sanctions policy.

Pupils who experience issues accessing appropriate apps / websites should report this to the Head of IT to have them unblocked through the school’s systems. This will in turn improve the wi-fi experience for other pupils.

10. MONITORING AND ACCESS

Pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

As stated in the parent contract, any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined under such circumstances. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

11. RETENTION OF DIGITAL DATA

Pupils must be aware that all pupil Microsoft 365 accounts including Microsoft Outlook email inboxes will generally be disabled after half a term and deleted within 1 term of that person leaving the school. All school computer (AD) accounts will be disabled upon departure from the school with accounts and files deleted within 1 term.

Any information from email folders that is necessary for the school to keep for longer, including personal information (e.g. for a reason set out in the school privacy notice), should be held on the relevant personnel or pupil file.

Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.
If you consider that reasons exist for the protocol not to apply or need assistance in how to retain and appropriately archive data, please contact the Bursary.

12. BREACH REPORTING

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, e.g., through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;

- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the ICO without undue delay (ie within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If pupils become aware of a suspected breach they should: notify a member of staff, ideally the DSL/e-safety Co-ordinator or Head of IT. Pupils should be prepared to co-operate with the documentation of breach details including: how long, what data & how far has the data got?

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

13. BREACHES OF THIS POLICY

A deliberate breach of this policy by pupils will be dealt with as a disciplinary matter using the school's usual applicable procedures. In addition, a deliberate breach by any person may result in the school restricting that person’s access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy or are concerned that a member of the school community is being harassed or harmed online, you should report it to the **Designated Safeguarding Lead** (in the case of concerns regarding online harassment or harm) or the **Bursar** (for any other concerns). Reports will be treated in confidence wherever possible.

ACCEPTANCE OF THIS POLICY

Please confirm that you understand and accept this policy by signing below and returning the signed copy to Marcia O’Mahony, Registrar.

I understand and accept this acceptable use of IT policy for pupils:

Signature: ____

Date: _______________________

Name: _____________________________________

For younger pupils (below secondary school age):

Parent’s Name: _____________________________________

Signature: ____

Date: _______________________

Part D: Bring Your Own Device (BYOD) Policy (Staff and Visitors)

GLOSSARY OF TERMS

Personal data	Any information that relates to an identified or identifiable living individual.
School data	Data held by and/or belonging to the school including but not limited to personal data held about pupils, staff and visitors.
Personal Device	Any piece of electronic equipment not provided by the school, purchased by an individual for their personal use including (but not limited to) mobile phones, tablets, laptops and desktop computers.
School IT Resources & Communication Systems	Any IT service provided by the school to its staff and pupils for school operations, including (but not limited to) Microsoft 365 accounts (Microsoft Outlook (school email), Microsoft Teams, OneDrive, SharePoint etc.), Windows Computer access and all school Wi-Fi networks.

We recognise that many of our staff and visitors have personal mobile devices (such as tablets, mobile phones and handheld computers), which they could bring to the school and, in the case of staff, use these devices for work purposes. However, the use of personal mobile devices within the school introduces increased risks in terms of the security of our IT resources and communication systems, the protection of confidential and proprietary information, and compliance with legal obligations (including child safeguarding).

This policy sets out rules on the use of personal devices in order to:

- protect our systems, as further defined below;
- protect school data (including personal data), as further defined below; and
- set out how we will manage and monitor your access to our systems.

Staff covered by this policy may use a personal mobile device for work purposes, subject to receiving prior written authorisation from the Bursar or Head of IT and adherence to the terms of this policy.

The school reserves the right to prohibit bringing personal devices into the school and/or using them for work purposes (as applicable). The school also reserves the right to require personal devices to be switched off at certain times and/or within certain areas of the school.

This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our:

- Acceptable Use of IT Policy for Staff (Part B of P2.6 E-Safety Policy Group),
- P90.5 Data Protection and Retention Policy,
- Social Media Policy (Located in the Staff Handbook under Section C: Communications & Information),
- P2.1 Anti-Bullying, Racial or Sexual Harassment Policy.

SCOPE AND PURPOSE OF THE POLICY

This policy applies to staff and visitors who use a personal mobile device including any accompanying software or hardware (referred to as a device in this policy) within the school and/or for work purposes. Note that it applies to use of the device for work purposes both during and outside school hours and whether or not use of the device takes place at school.

For staff, this policy applies to all devices used to access our IT resources and communication systems (collectively referred to as **systems** in this policy), which may include (but are not limited to) mobile phones, tablets, and laptop or notebook computers.

When you access our systems, you may be able to access data about the school, including information which is confidential, proprietary or private (collectively referred to as **school data** in this policy).

As part of granting your personal device access, the school will take steps to keep your personal device's wider data and systems separate from our systems and school data which you access from that device.

When you access our systems using a device, we are exposed to several risks, including from the loss or theft of the device, the threat of malware and the loss or unauthorised alteration of school data. Such risks could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy. This could also result in damage to our systems, our business and our reputation.

Breach of this policy may lead to us revoking your access to our systems, whether through a device or otherwise. It may also result in disciplinary action up to and including dismissal. Disciplinary action may be taken whether the breach is committed during or outside school hours and/or whether or not use of the device takes place at school. You are required to co-operate with any investigation into a suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.

Relatedly, this policy also applies to visitors (and staff) who access our wireless networks on their own devices for personal use (see further below).

SECTION A: STAFF

1. ACCESS TO OUR WIRELESS INTERNET NETWORKS

We provide a wireless network that you may use to connect your device to the internet. Access to the wireless network is at the discretion of the school. It should under no circumstances be used to access or distribute content that is unlawful, harmful, explicit, offensive or otherwise inappropriate. We may withdraw access from anyone we consider is using the network inappropriately.

The wireless network **YMS-SCHOOL** is available for staff to use to connect personal devices to the internet. In order to use YMS-SCHOOL staff must download & install our Wi-Fi Certificate on to all devices that require internet access. School login details are then able to be used to login to the network and verify identity.

Access to the wireless network should under no circumstances be used to access or distribute content that is unlawful, harmful, explicit, offensive or otherwise inappropriate. We may withdraw access from anyone we consider is using the network inappropriately.

We cannot guarantee that the wireless network is secure, and you use it at your own risk. In particular, you are advised not to use the wireless network for online banking or shopping.

The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto your own device whilst using our wireless network. This activity is taken at your own risk and is discouraged by the school. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's wireless network.

The school may use technology that detects and monitors the use of mobile and other electronic or communication devices which are connected to or logged on to our wireless network. By using a mobile device on the school's wireless network, you agree to such detection and monitoring.

The information that we may monitor includes (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites and information uploaded to or downloaded from websites.

Staff should also refer to the Monitoring section below for further information.

2. IMAGES AND RECORDINGS

You are not permitted under any circumstances to use your personal devices when taking images, videos or other recording of any pupil nor to have any images, videos or other recording of any pupil on your personal devices. Please read this in conjunction with the Social Media Policy (see Staff Handbook), P2.2 Safeguarding and Child Protection Policy, Acceptable Use of IT Policy (Section B of this policy group) and P2.3 Staff Code of Conduct.

3. MONITORING (STAFF USING SYSTEMS)

The contents of our systems and school data are our property. All materials, data, communications and information, including but not limited to e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device (collectively referred to as content in this policy) during the course of business or on our behalf is our property, regardless of who owns the device.

We reserve the right to monitor, intercept, review and erase, without further notice, all content on the device that has been created for us or on our behalf. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, logins, recordings and other uses of the device, whether or not the device is in your possession.

It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. You should have no expectation of privacy in any data on the device. Staff are advised not to use our systems for any matter intended to be kept private or confidential and to avoid processing any personal data relating to non-school related third parties (for example, your family and friends) on our systems.

Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law in order for us to comply with a legal obligation or for our legitimate school purposes, including, without limitation, in order to:

- prevent misuse of the device and protect school data;
- ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy);
- monitor performance at work; and
- ensure that staff members do not use our facilities or systems for any unlawful purposes or activities that may damage the school, its systems or reputation.

We may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. We may obtain and disclose copies of such content or of the entire device (including personal content) for litigation or investigations.

You acknowledge that the school is entitled to conduct such monitoring where it has a legal obligation or legitimate basis to do so, and that (without further notice or permission) we have the right to copy, erase or remotely wipe the entire device (including any personal data stored on the device).

Whenever we monitor personal data it will be carried out in line with government guidance such as KCSIE. This is also set out in the school's Staff Privacy Notice. You acknowledge that you use the device at your own risk and that we will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.

4. SECURITY REQUIREMENTS

You must comply with the Acceptable Use of IT Policy (Section B of this policy group) when using your device to connect to our systems.

In addition to the requirements set out in the above-mentioned policies and set out above in this policy, you must also:

- in no circumstances use your personal email or other personal messaging account to transfer, attach, discuss, or otherwise use school data or any other information which may be contained in our systems. To the greatest extent technically possible, our systems and our data must be kept separate from the rest of your personal device;
- install any anti-virus or anti-malware software at our request before connecting to our systems and consent to our efforts to manage the device and secure our systems and school data, including providing us with any necessary passwords;
- protect the device with a PIN or strong password and keep that PIN or password secure at all times. If the confidentiality of a PIN or password is compromised, you must change it immediately;
- not download or transfer any school data to the device, for example via e-mail attachments, unless specifically authorised to do so. Staff must immediately erase any such information that is inadvertently downloaded to the device;

If a staff member is unsure or not confident that their device meets all of the above criteria or is too old to receive the latest software update, the school strongly advises that the device is not used for work purposes. If a staff member is not confident in how to best keep their personal data and school data separate, the school strongly advises that the device is not used for work purposes.

We reserve the right, without further notice or permission, to inspect your device and access all school data and applications on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the school data on it for legitimate business purposes.

If we discover or reasonably suspect that there has been a breach of this policy, including any of the security requirements listed above, we shall immediately remove access to our systems and, where appropriate, remove any school data from the device. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from school data in all circumstances. You should regularly backup any personal data contained on the device.

You acknowledge that, without further notice or permission, we may need to inspect a device and applications used on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the data on or from a device for legitimate purposes.

5. LOST OR STOLEN DEVICES AND UNAUTHORISED ACCESS

In the event of a lost or stolen device, or where a staff member believes that a device may have been accessed by an unauthorised person or otherwise compromised, the staff member must report the incident to the Head of IT immediately.

Appropriate steps will be taken to ensure that school data on or accessible from the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all school data on the device (including information contained in a work e-mail account, even if such e-mails are personal in nature). As noted above, although we do not intend to wipe other data that is strictly personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from school data in all circumstances. You should regularly backup all personal data stored on the device.

6. USE OF EXTERNAL HARDDRIVES / STORAGE DEVICES

Some staff may have historic teaching materials stored on external harddrives (HDD or SSD) which they use for . Staff must ensure that care is taken to:

- Ensure no personal data belonging to the school is stored on harddrives, this includes the personal data of pupils, staff and others
- Ensure harddrives are kept secure (password protected / encrypted)
- Harddrives are protected against theft

7. PROCEDURE ON TERMINATION OF EMPLOYMENT

On your last day of work, all school data (including work e-mails), and any software applications provided by us for work purposes, will be removed from the device. If this cannot be achieved remotely, the device must be submitted to the Head of IT for wiping and software removal. You must provide all necessary co-operation and assistance in relation to this process.

8. PERSONAL USE

We have a legitimate basis or legal obligation to access and protect school data stored or processed on your device, including the content of any communications sent or received from the device. Where we are relying on our legitimate interests, we recognise the need to balance our need to process data for legitimate purposes, with your expectations of privacy in respect of your personal data. Therefore, when taking (or considering taking) action to access your device or delete data on your device (remotely or otherwise) in accordance with this policy, we will, where practicable:

- consider whether the action is proportionate in light of the potential damage to the school, its pupils or other people impacted by school data;
- consider if there is an alternative method of dealing with the potential risks to the school's interests (recognising that such decisions often require urgent action);
- take reasonable steps to minimise loss of your personal data on your device, although we shall not be responsible for any such loss that may occur; and
- delete any such personal data that has been copied as soon as it comes to our attention (provided it is not personal data, which is also school data, including all personal emails sent or received using our email system).

As noted above, it is important to separate your personal data from school data. To reduce the likelihood of the school inadvertently accessing your personal data, or the personal data of third parties, you must comply with the following steps to separate school data from your personal data on the device:

- do not use work e-mail for personal purposes, but if you do ensure that it is labelled appropriately in the subject line;
- regularly backup all personal data stored on the device;

9. APPROPRIATE USE

You should never access or use our systems or school data through a device in a way that breaches any of our other policies, in particular our Acceptable Use of IT Policy (Section B of this policy group) and P90.5 Data Protection and Retention Policy. If you breach any of the above policies, you may be subject to disciplinary action up to and including dismissal.

You should also minimise the amount of school data you retain on the device by accessing information remotely where possible, and deleting any data saved locally on your device as soon as it is no longer require (the ideal default position is that this concern should not be possible at all).

You must not talk, text, e-mail or otherwise use a device while operating a school vehicle or while operating a personal vehicle for school purposes. You must comply with any applicable law concerning the use of devices in vehicles.

10. SEPARATION OF DATA

We acknowledge that some staff work for multiple organisations and therefore their personal devices may have access to multiple organisation's data including the schools. It is the staff member's responsibility to ensure separation of different organisations data as well as separation from personal data is maintained. This can be achieved by the use of separate email applications for each individual organisation or personal account to ensure data is not shared across the different accounts.

Any breach or suspected breach of this separation should be reported immediately in line with our P90.5 Data Protection and Retention Policy. Should another organisation require access to your device, the school should be notified to ensure privacy of the school's data can be appropriately maintained.

SECTION B: VISITORS

1. ACCESS TO OUR WIRELESS INTERNET NETWORKS

Visitors to the school are invited to join the **YMS-GUEST** network. Access to the wireless network is at the discretion of the school. It should under no circumstances be used to access or distribute content that is unlawful, harmful, explicit, offensive or otherwise inappropriate. We may withdraw access from anyone we consider is using the network inappropriately. Visitors to the school who are hiring the school site may be provided with access to additional school networks for the duration of their hire.

Guests should **under no circumstances** share the provided password for **YMS-GUEST** with other YMS guests, staff or **pupils**. This includes both verbally, written, or via digital password sharing.

We cannot guarantee that the wireless network is secure, and you use it at your own risk. In particular, you are advised not to use the wireless network for online banking or shopping.

The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto your own device whilst using our wireless network. This activity is taken at your own risk and is discouraged by the school. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's wireless network.

The school may use technology that detects and monitors the use of mobile and other electronic or communication devices which are connected to or logged on to our wireless network. By using a mobile device on the school's wireless network, you agree to such detection and monitoring.

The information that we may monitor includes (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites and information uploaded to or downloaded from websites.

2. IMAGES AND RECORDINGS

You are not permitted under any circumstances to use your personal devices when taking images, videos or other recording of any pupil nor to have any images, videos or other recording of any pupil on your personal devices. Please read this in conjunction with the Social Media Policy (see Staff Handbook), P2.2 Safeguarding and Child Protection Policy, Acceptable Use of IT Policy (Section B of this policy group) and P2.3 Staff Code of Conduct.

WHO IS RESPONSIBLE FOR THIS POLICY?

The Bursar in conjunction with the Head IT shall have overall responsibility for the effective operation of this policy and shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice. If you have any questions about this policy or other queries related to use of your own device for work purposes please contact the Bursar or the Head of IT.

Part E: AI Policy

1. STATEMENT OF INTENT

Artificial Intelligence (AI) technology is already widely used in commercial environments and is gaining greater use in education. We recognise that the technology has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff in reducing workload. We also realise that there are risks involved in the use of AI systems, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address AI risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which AI technologies are likely to play an increasing role.

The safeguarding of pupils will, as always, be at the forefront of our policy and practice.

There are currently 3 key dimensions of AI use in schools:

- learner support
- teacher support, and
- school operations;

ensuring all use is safe, ethical and responsible is essential.

2. RELATED POLICIES

This policy forms the primary reference for guidance on how AI can be used by staff at the Yehudi Menuhin School, however more specific guidance about how AI may be used in specific area of the school can be found in the policies listed below. This policy should be read in conjunction with these other school policies:

- P90.5 Data Protection and Retention Policy
- Staff Handbook
- P2.3 Staff Code of Conduct
- P3.0 Behaviour Management policy
- P2.1 Anti-bullying, Racial or Sexual Harassment policy
- P2.6 E-Safety Policy Group including:
    - Staff E-Safety Policy: Keeping Pupils Safe Online
    - Acceptable Use of IT Policy for Staff
    - E-Safety Guidance & IT Acceptable Use Policy for Pupils
    - Bring your own device (BYOD) Policy for Staff & Visitors
- P1.1 Curriculum Policy
- P1.4 Equal Opportunities policy

3. POLICY STATEMENTS

The school acknowledges the benefits of the use of AI in an educational context - including enhancing teaching and learning outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.

We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.

We will ensure that, within our education programmes, learners understand the ethics and use of AI and the potential benefits and risks of its use. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.

As set out in our IT acceptable use agreements (Part B: Acceptable Use of IT Policy for Staff & E-Safety Guidance & Part C: E-Safety Guidance and IT Acceptable Use Policy for Pupils), the school will use AI responsibly and with awareness of data sensitivity. Where used, staff should use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.

Staff should always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.

Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.

We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.

The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.

AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the Data Protection Lead and the Head of IT. Quick reporting helps mitigate risks and facilitates a prompt response.

We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.

The school will support parents and carers in their understanding of the use of AI in the school through our Letter to Parents about Technology which can be found as an appendix in our E-Safety Policy Group and is sent out to parents at the start of each school year.

AI tools may be used to assist teachers in the assessment of learner's work and identify areas for improvement. Teachers may also support learners to gain feedback on their own work using AI. Use of these tools should be purposeful, considered and with a clear focus on ensuring impact and understanding and mitigating risk.

Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.

We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.

Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Code of Conduct.

4. RESPONSIBILITIES

All staff are responsible for being the human in the loop (HITL) when it comes to the use of AI in Education. HITL is the safeguard that ensures there is always an accountable human where AI is being used, this role includes reviewing the decisions AI makes, being prepared and informed to answer questions from pupils, parents and visitors about how the school is choosing to use AI ethically and the continued responsibility to safeguard pupils from harm.

Head and Senior Leaders

Are responsible for the strategic planning of how AI will be used in the school, establishing AI policies and procedures and ensuring that all staff receive relevant training and have a clear understanding of these.

Designated Safeguarding Lead

Our Designated Safeguarding Lead has responsibility for online safety in the school. They are expected to have knowledge of AI and its safeguarding implications and an in-depth working knowledge of key guidance. We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

Data Protection Lead

The DPL will be responsible for providing advice and guidance about data protection obligations in relation to the use of AI, including related Data Protection Impact Assessments (DPIAs).

Technical Staff

The Head of IT supported by the school's external IT support provider, EducAite, will be responsible for technical support and guidance, with particular regard to cyber-security and the effectiveness of filtering and monitoring systems. The Head of IT will ensure the external IT support provider is aware of the school's requirements regarding AI and comply with school policies.

Staff

It is the responsibility of all staff to have read and understood this policy and associated Acceptable Use Agreements. All staff must report any incidents or suspected incidents concerning the use of AI in line with school policy. All staff will challenge any inappropriate behaviour. Staff have a duty to ensure that:

- the school environment is safe
- sensitive and confidential data / information is secure
- that their actions do not put the reputation of the school at risk and that
- learners understand their responsibilities

Governors

We ensure that our governing body has a good understanding of how AI is used in a school context and potential benefits and risks of its use. They receive regular updates, enabling them to support the school and challenge where necessary. This may include evaluation of the use of AI in the curriculum, administration and communications, ensuring that risks relating to these issues are identified, that reporting routes are available, and that risks are effectively mitigated.

Parents/carers

Our parents and carers are made aware of how AI is used in school and receive guidance on both good practice in its use and the risks of misuse that may affect their children's learning or safety. They are encouraged to report any concerns to the school and are made aware that all incidents will be handled with care and sensitivity.

5. VULNERABLE GROUPS, BIAS AND DISCRIMINATION

We recognise that vulnerable learners are more likely to be at risk from the misuse of AI (both in their own use or through the actions of others). We ensure that vulnerable learners are offered appropriate support to allow them to gain full benefit of the use of AI, while being aware of the potential risks.

Children are considered to be vulnerable data subjects and therefore any process involving their personal data is likely to be "high risk". If an AI/ automated process is used to make significant decisions about people, this is likely to trigger the need for a Data Protection Impact Assessment (DPIA).

Due to the known biases that can be present in AI-generated suggestions, AI will never be used by the school in decision-making around pupil applications to the school or job applications made by potential future employees.

6. REPORTING

- Our reporting systems are well promoted, easily understood and easily accessible for staff, learners and parents/carers to confidently report issues and concerns, knowing these will be treated seriously. All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties. This can be done via our established school reporting mechanisms.

7. RESPONDING TO AN INCIDENT OR DISCLOSURE

Our response is always based on sound safeguarding principles and follows school safeguarding and disciplinary processes. It is calm, considered and appropriate and puts the learner at the centre of all decisions made.

- All AI incidents (including data breaches and/or inappropriate outputs) must be reported promptly to the Data Protection Lead and the Head of IT. Effective reporting helps mitigate risks and facilitates a prompt response.
- Where relevant / required incidents will be reported to external agencies e.g., Police, LADO, DPO, ICO.
- All AI related incidents will be recorded through the school's normal recording systems

In the case of misuse of AI by staff, the normal staff disciplinary processes will be followed.

8. RISK ASSESSMENT

It is key that our approach to managing risk aligns with, and complements, our broader safeguarding approach.

The school understands that despite many positive benefits in the use of AI, there are some risks that will need to be identified and managed, including:

- Legal, commercial, security and ethical risks
- Data Protection
- Cyber Security
- Fraud
- Safeguarding and well-being
- Duty of care

9. EDUCATION

Our school's educational approach seeks to develop knowledge and understanding of emerging digital technologies, including AI.

This policy outlines our commitment to integrating Artificial Intelligence (AI) responsibly and effectively within our school environment. We will use AI responsibly, safely and purposefully to support these aims:

- Enhance academic outcomes: Improve educational experiences and performance for pupils.
- Support teachers: Assist in managing workloads more efficiently and effectively.
- Educate on AI use: Promote safe, responsible, and ethical AI practices among staff and learners.
- Develop AI literacy: Incorporate AI as a teaching tool to build AI skills and understanding.
- Prepare for the future: Equip staff and pupils for a future where AI is integral.
- Promote educational equity: Use AI to address learning gaps and provide personalised support.

In light of the risks and challenges of AI, the introduction and use of AI systems in the classroom should meet the following benefits and requirements:

- Approved by Deputy Head (Academics) and Data Protection Lead (Bursar) A full list of previously approved systems can be requested from the Head of IT
- Use of AI will provide pupils with an opportunity for learning that could not be achieved with other existing pedagogical methods
- Use of AI will improve learning outcomes
- Pupils' use and engagement with AI can be monitored by staff in the classroom
- AI output can be monitored, checked and verified by teachers
- Staff member delivering AI-based lesson is confident in discussing the ethical and safe use of AI with pupils
- AI outputs can be clearly labelled

- Staff should be confident that pupils will be able to use the AI to work alongside them to promote and support their learning, not provide opportunities for shortcuts

10. TRAINING

As AI becomes an integral part of modern education, it is essential for staff to be trained in its effective use. Training equips educators with the knowledge and skills to integrate AI tools responsibly into teaching, learning, and administrative processes. It ensures that AI is used to enhance educational outcomes, streamline workloads, and promote equity while safeguarding ethical practices and data privacy. By fostering AI literacy, staff can confidently prepare pupils for a future where AI is a key driver of innovation and opportunity.

- We will provide comprehensive training to all staff on the effective, responsible, and ethical use of AI technologies in education, ensuring these tools enhance teaching, learning, and administrative processes.
- We will integrate AI-related risks and safeguards into annual safeguarding training, aligning with statutory guidance
- We will ensure all staff are equipped with the knowledge and skills to confidently integrate AI into their professional practice and to prepare pupils for a future shaped by AI-driven innovation and opportunities.
- We will train staff to identify, assess, and mitigate risks associated with AI technologies, including issues such as biased algorithms, privacy breaches, and harmful content.
- We will train staff on robust data protection practices, ensuring compliance with UK GDPR and other relevant regulations while using AI systems.
- We will promote ethical practices in the use of AI, ensuring that these technologies contribute to equity, fairness, and inclusivity in education.
- We will empower educators to teach learners about the safe and ethical use of AI, cultivating a culture of awareness, resilience, and informed decision-making in the digital age.
- We will train staff to use AI responsibly as a tool to monitor and address online risks, reinforcing our commitment to a safe learning environment.

All Staff have access upon request the *9ine Platform LMS Academy: AI Pathway* which provides both fundamental beginner courses to understand AI as well as advanced and specialist courses for school leaders and IT strategists. Available training:

Beginner

- AI in Education: Introduction to AI (Beginner)
- AI in Education: Introduction to Ethics and AI (Beginner)

Intermediate

- AI in Education: Ethics and AI in Practice (Intermediate)
- AI in Education: EdTech and Vendor Management (Intermediate)

- AI in Education: Leadership and Governance (Intermediate)
- AI in Education: Risk management (Intermediate)

Advanced

- AI in Education: Ethics and AI in Practice (Advanced)
- AI in Education: EdTech and Vendor Management (Advanced)
- AI in Education: Policies and Procedures (Advanced)
- AI in Education: Individual Rights (Advanced)
- AI in Education: Leadership and Governance (Advanced)
- AI in Education: Risk management (Advanced)
- AI in Education: Privacy (Advanced)
- AI in Education: Cybersecurity (Advanced)
- AI in Education: ICT/Data Management (Advanced)
- AI in Education: Training/Communications (Advanced)

Specialist

- AI in Education: AI for Safeguarding (Specialist – DSL/Safeguarding Lead)
  AI in Education: Privacy (Specialist – Data Privacy & Protection leads)
- AI in Education: Cybersecurity (Specialist – IT Managers)
- AI in Education: ICT/Data Management (Specialist – IT Managers & Strategy leads)
- AI in Education: Ongoing Management (Specialist – School leaders)

Appendix A: Letter to Parents about Technology

As part of our role of developing 21st Century musicians, we endeavour to nurture pupils who are confident and comfortable with their use of technology, aiming for balance and an understanding of the importance of switching off and disconnecting daily. Whilst technology can be a valuable tool for research and learning it is vitally important, we teach the dangers and potential risk of exposure to harmful and unwanted content, as well as the risks to wellbeing of social media, online criticism and the importance of protecting personal data.

1. Preparing for YMS

Laptops/Tablets

Pupils are required to bring with them a device suitable for completing their school work.
Suitable devices must:

- Be compatible with Microsoft 365, with Windows Laptops being the most reliable devices.
- Not be Google Chromebooks, these are not a suitable device for YMS.
- have a suitable keyboard attachment and mouse or trackpad
- have Microsoft Outlook, Microsoft Teams and Microsoft OneDrive applications installed
- not still be connected / managed by the pupil's previous school

All pupils are provided by the school with a school email address which gives them access to their Microsoft 365account which should be logged in on their device. Their account provides access to a wide range of Microsoft applications which support them in their studies.

Mobile Phones

The school provides Wi-Fi that is filtered and monitored by the school's Safeguarding team allowing us to investigate any concerns we may have about what your child is attempting to access.

There are however by-passes that stop the school from effectively delivering this Safeguarding. Pupils with large amounts of mobile data often by-pass the school's monitoring by using their data and tethering/hot spotting their other devices. Parents must be aware that there is no possible way for the school to monitor mobile data usage and consider putting data caps on pupil's data usage. parents **must be aware** that the school has **no control** over pupils browsing over 3G/4G/5G (using mobile data). Mobile data connects directly to your child's mobile phone provider bypassing the school's protective layers. This also means data is not affected by the timing restrictions put in place by the school (meaning pupils can access the internet after 11pm).
Whilst having some data is useful for when pupils are travelling off-site, we highly recommend parents keep a cap on data usage, encourage pupils to use the school

Wi-Fi to access the internet and, particularly for younger pupils, consider putting further restrictions in place – please see below for tips for controlling pupil data usage.

If your child experiences issues with the school Wi-Fi please report their issues to the school's Head of IT. Issues around blocked apps / websites can be resolved if communicated to the school. Pupils are also encouraged to do this themselves via Teams. We understand parents wanting to solve these issues for their child, however providing mobile data drastically reduced the school's ability to safeguard your child when online.

International parents should purchase a UK-Sim for pupils to use whilst in the UK. The benefit of this is that should pupils need to contact the school duty mobiles outside of "Wi-Fi" hours (06:00-23:00) or whilst off-site, they can do so without the concern of having high call-charges or having to use data.

If you have bought a phone on contract, there is a high chance it is "SIM-locked" meaning it will only work with a sim card from that specific network service provided. If the contract has ended, you should be able to request the phone is unlocked. Phones must be unlocked to work with a foreign SIM card.

Please note: not all USA mobile phones will work abroad, please speak to your provider if you are unsure.

VPNs (Virtual Private Network)

VPN or Virtual Private Networks create a private connection between a users device and a remote server which then connects to the Wi-Fi network on your behalf. Remote servers can be based in another country, allowing you to appear as if you are in that country when browsing the internet, however it stops a network from being able to identify your device. This is very helpful when connected to public networks (such as trains, cafes, airports) however is not appropriate in a school environment where our role is to monitor and protect our pupils.

VPNs are another method of by-passing the school's ability to identify Wi-Fi users. VPN usage can often be the cause of or hide Wi-Fi issues. It has been identified that pupils often use VPNs to try and avoid issues with school Wi-Fi rather than reporting the issue, which then protracts it.

Parental Controls

We highly recommend parents of pupils under the age of 14 have in place parental controls on to their child's devices such as screentime and restrictions on the download of apps.

HOWEVER, parents must be aware pupils may need their consent to download and install applications needed for school, and so any controls put in place must be compatible your child being away at school. For example, some parental controls require proximity to the parents device which can cause issues when away from your child.

Screen time restrictions are encouraged but exemptions should be put in place for school applications such as Microsoft Teams.

School Controls
Pupils aged 14 and below (C-age students) hand their devices in every weekday and Sunday evening at 9pm, 30 minutes before their bedtime and for those pupils who are not required to hand their devices in, the Wi-Fi turns off at 11pm and comes back on at 6am.

The school provides site-wide access to Wi-Fi (wireless internet access) which they can connect to using their school computer logins. The Wi-Fi has several layers of protection including a filtering system in additional its firewall which ensures harmful/unwanted content is blocked.

2. School Accounts

Pupils' YMS accounts provide them with access to both download of the Microsoft 365 Suite (Outlook, OneDrive, Word, PowerPoint, Excel) on to a device of their choosing as well as access to the web version of these apps. **If the pupil already has a Microsoft login (either personal or from a previous school) we highly recommend they are logged out.** Microsoft does allow for switching between a personal and school account, but this can become problematic if the pupil forgets to switch and accidentally shares a file with their teacher from a personal account.

Pupils are required to store all their schoolwork in their school OneDrive. This cloud-based drive storage protects against file loss in the event the device is damaged/stolen and frees up space on the device which aids connectivity speed.

All communication between pupils and school staff must take place using their @menuhinschool.co.uk Microsoft account.

All pupils over the age of 11 are required to have Microsoft Teams downloaded on to their mobile phones, as this is the main means of communication between pupils and boarding staff (this includes day pupils). We also recommend pupils have access to their Outlook email inbox and check it regularly.

As well as their email login, the school also provides pupils with a computer login, to login and access the school's printers. The same login also provides access to the school's Wi-Fi network.

It is pupils' responsibility to keep their accounts secure and advice on creating safe and secure passwords can be found in the school's IT Acceptable Use Policy, which all pupils are required to read and agree to.

3. Communicating with Staff

No staff member should have a pupil's personal phone number/email address and Microsoft Teams provides an easy and safe way for pupils and staff to communicate during term-time. Boarding staff have access to and store all pupils' mobile numbers on the House Duty mobiles (Cowan House 07884 311 548 / Harris House 07884 311 868) which are secure school devices. Parents may also contact house staff on these numbers. Pupils should never have personal contact information for staff and should contact staff only through formal school channels. This also applies to parents.

Where possible pupils and staff should not be communicating beyond the end of the school day.

Pupils should not communicate with staff via social media, and it is not appropriate to add staff on social media such as Facebook/WhatsApp/WeChat. From an artistic perspective we understand pupils may wish to follow staff (particularly Music staff) on their professional accounts, however staff are not permitted to follow them back. Pupils should under no circumstances use this as a way to communicate with staff. YMS alumni should not be accepted as a friend on Facebook until they have left YMS for three full academic years.

Please note: WhatsApp is a 13+ app and the school therefore strongly discourages all pupils under 13 from using this application. Under absolutely no circumstances should pupils be communicating with YMS staff via this app as it clearly violates the rule about staff and pupils being in possession of each other's personal phone numbers. To support this, the Cowan House and Harris House duty mobiles ceased usage of the application completely in 2021.

WeChat is a 13+ app and the school therefore strongly discourages all pupils under 13 from using this application. Pupils between 13-18 must have parent/guardian permission to use this app. The Cowan House and Harris House duty phone do not use this app for communication.

4. Monitoring Use of IT

The School filters and monitors pupils' use of the School internet network via SOPHOS filtering and monitoring systems. Alerts about inappropriate activity are sent automatically to the Deputy Head (Pastoral), and the School will not hesitate to take action against pupils viewing, or attempting to view, inappropriate websites using the School network. This may include conducting a search of pupils' devices.

5. Mobile Phones & UK-Sims

All pupils must be contactable on their mobile phones via Microsoft Teams; therefore, all pupils must have a mobile device appropriately compatible with the latest version of Microsoft Teams.

Please check here for the latest hardware requirements for the Team application:
Hardware requirements for Microsoft Teams - Microsoft Teams | Microsoft Learn

Updated January 2023:

You can use Microsoft Teams on these mobile platforms:
Android (e.g. **Samsung**): Compatible with Android phones and tablets.
Support is limited to the last four major versions of Android. For example, when a new, major version of Android is released, the Android requirement is the new version and the three most recent versions that precede it.
iOS (**Apple**): Compatible with iPhone, iPad, and iPod touch.
Support is limited to the two most recent major versions of iOS. For example, when a new, major version of iOS is released, the iOS requirement is the new version and the most recent versions that preceded it. The optional Blur my background video effect on iOS requires an operating system of iOS 12 or later, compatible with the following devices: iPhone 7 or later, iPad 2018 (6th generation) or later, and the iPod touch 2019 (7th generation).

We understand that mobile phones play a vital and important role in communicating with your children whilst they are away from you at school, especially for international parents who have less frequent opportunities to visit during term time. The school asks for parents' support in encouraging a healthy lifestyle, including turning off devices at night. Owing to time zones, we understand it can be challenging to find times during the day to speak to children with busy school/work schedules, however the school asks for parents' support in encouraging pupils not to stay up late to make calls. The school Wi-Fi turns off at 23:00 every evening to encourage sensible and appropriate usage by pupils.

Pupils have morning break (10:30 GMT/BST), lunchtime (12:15-14:15 GMT/BST) and afternoon break (16:30 GMT/BST) during which it might be more convenient to set up a regular time to call.

It is also important to note, that whilst away from home staff are here to support pupils' pastoral needs. Having a direct line to your child could mean important information bypasses house staff and we encourage parents to keep house staff fully informed about events at home which may present challenges to pupils.

6. Wi-Fi Restrictions

On occasion, pupils may find a website they would like access to is blocked and are encouraged to notify the IT staff on-site (via Teams) with a link to the website to review and unblock the website for them if appropriate.

Below are a list of common applications and whether pupils will be able to access them on school Wi-Fi:

Allowed?	**Application**	**Use**	**Reason for decision**
Yes	WhatsApp	Social network / Communication	Many of our international pupils use WhatsApp as a way to communicate with home.
Yes	WeChat	Social network / Communication	Many of our international pupils use WeChat as a way to communicate with home.
Yes	Telegram	Social network / Communication	Many of our international pupils use Telegram as a way to communicate with home. Recommend using security features available in the app to limit who can

			add them to group chats & who their mobile number is visible to.
Yes	Duolingo	Education	Language learning app
No	Tiktok	Social network / Communication	By default, all accounts are public, potential to connect with strangers.
No	SnapChat	Social network / Communication	Realtime location sharing. Easy to connect with strangers.
No	TEMU	E-commerce	Intended for 18+. Sells items for children but for sale to adults.
No	Steam	Gaming	Easily access age-inappropriate games without parental controls in place.
No	Pinterest	Social network / Communication	Potential to connect with strangers, potential to search for inappropriate/negative content

As part of an annual review of the school's IT policies, a committee meets annually to review and approve the current filtering on the school's network. Students and staff are also able to raise any issues they have with over-blocking or access to usually restricted content for educational purposes by contacting the IT team and will be reviewed on a case-by-case basis.

7. Tips for controlling pupil data usage

Parents are requested to ensure that settings are applied to restrict usage when pupils should be asleep or otherwise protected from screen time.

Use Parental Controls to Keep Your Child Safe | NSPCC

Use parental controls on your child's iPhone, iPad and iPod touch – Apple Support (UK)

8. Additional devices

We advise that pupils do not bring more than two devices with them (including their mobile phone) (Kindles do not count as an additional device). Portable games consoles are acceptable, however please notify house staff about this and consider ensuring the usage is limited.

Pupils' second device should be a portable computer which can be used to support their academic learning.

Minimum portable computer specifications:
CPU: i5 (Intel) / A10 (AMD)
8GB RAM / 16GB RAM (recommending if using for composition software)
256 / 512GB SSD (storage)

We do not recommend Chromebooks for use at YMS. We are a Microsoft based school and find Google devices are frequently incompatible with school systems.

We understand that not all parents are able to provide students with a new device, and therefore the school offers a programme to loan pupils devices for the duration of their time at the school. To discuss this option and apply for the Pupil Device loan scheme, please contact niamh.poole@menuhinschool.co.uk.

The school's internet and devices are protected by a combination of a firewall for security, and an additional layer of age-appropriate filtering. Both are provided by SOPHOS and are managed by EducAite, our IT support providers.

9. Use of AI in school

The school recognises the growing use of AI (Artificial Intelligence) and aims to equip our pupils with the knowledge and skills to use AI in an ethical and responsible way that will benefit them in a changing technological landscape whilst educating pupils about both the ethical and safety risks associated with use of AI.

Pupils' use of AI should come from a place of intellectual curiosity and creativity with a goal of supporting their own learning. They should engage in open dialogue with teachers about how AI can support their learning and aim to understand why certain usage is discouraged/restricted.

A full list of guidance for pupils around the use of AI has been added to the IT Acceptable use policy (for pupils) and parents are encouraged to read and support their children to understand the school's approach to AI.

An overview of the school's approach is below:

- **Personal Data:** the school is aware of its responsibility as a data controller and is aware that the personal data it holds should remains within the schools' control. Staff and pupils are taught about the risks of entering personal data including images / videos / audio recordings into third-party AI tools.
- **Educational Benefits:** the school recognises that in a changing technological landscape, it is important for pupils to be equipped with new tools that can benefit their learning and future careers. However, pupils must recognise that excessive/inappropriate use of AI in their school work could be detrimental to their learning**,** through over reliance on AI obstructing the development of skills and resulting in difficulties for teachers to assess pupils' learning.
- **Transparency:** Pupils should be clear with teachers where and when they have used AI to support their academic work and in return teachers should be clear about when AI is being used to prepare class materials and provide feedback
- **Exams:** Pupils must not use AI to complete coursework or other exam materials.
  The school cannot shield pupils who are caught using AI in their exam subjects.
- **Critical Thinking:** Pupils must remain aware that AI chatbots are designed to seem friendly and approachable, however are no replacement for real human interaction and advice. They must learn to think critically about where information has come from and verify sources for accuracy.

- **Human in the Loop:** Any use of AI by school staff will always be checked for accuracy and bias by a member of staff. Decisions around pupils will never be made by a computer.

Please sign here to confirm you have read and understood the school's Technology Guidance and state below which devices your child will be bringing with them:

Parent/Guardian 1: ______________________________ ________________

Signature **Date**

Parent/Guardian 2: ______________________________ ________________

Signature **Date**

My child will be bringing with them:

	Brand **e.g. APPLE / SAMSUNG / HUAWEI**	**Type** **e.g. iPHONE 10 / GALAXY A13**	**Phone number**
Mobile Device:			
Laptop:			
Additional Devices:			

Glossary of Terms

Mobile Data (Cellular Data): Mobile data is internet content delivered to mobile devices such as smartphones and tablets over a wireless **cellular** connection.

Data Roaming: When you are traveling abroad, data roaming will take over from your mobile data. It allows you to access the internet in other countries. Keep in mind that data roaming will cost you extra.

Wi-Fi (Wireless Fidelity): Internet access without wires/cables.
Difference between Wi-Fi & Mobile Data: Wi-Fi is limited to being within range of a Wireless router / Access Point (AP) whilst Mobile data is limited only by your phone signal and therefore your phone network provider's coverage. Data transmitted over Wireless is limited by the quality of the router and your phone. Mobile data can be controlled with data caps through your phone plan.

Network/Mobile Network: (the mobile network infrastructure in the UK is owned by four mobile operators: O2, EE, Vodafone and Three. Any other mobile network will pay one of these companies to use the infrastructure and therefore the service will be cheaper but not necessarily as good. In the school's local area, we find O2 or Three seems to work best.)

Microsoft 365: a product family of Microsoft software including Office apps, cloud services and security solutions.

Microsoft Office Suite: the family of Microsoft products that includes:

Microsoft Word (written documents)
Microsoft PowerPoint (presentations)
Microsoft Excel (spreadsheets)
Microsoft Outlook (emails, contacts & calendars)
Microsoft OneNote (digital notebook)
Microsoft OneDrive (cloud-based drives for saving files)
Microsoft Teams (communication hub for messaging, document sharing, group working, video calling)