The Yehudi Menuhin School

E-Safety Policy Group

Incorporating:

Staff E-Safety Policy – Keeping Pupils Safe Online
Acceptable Use of IT Policy for Staff,
Acceptable Use of IT Policy for Pupils,
E-Safety Guidance for Pupils

Contents

Summary of material changes since the previous version

This policy has been updated to reflect the latest developments in technology, remote learning, and statutory guidance, including KCSiE 2023. The format has been changed to incorporate previously separate documents regarding Acceptable Use of IT and Guidance for Pupils.

Abbreviations, Acronyms and Definitions

Abbreviation / Acronym	Definition
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
Parents	Adults with parental authority for a child
Plagiarism	The act of taking someone else's work and passing it off as one's own.
PSHE	Personal, Social, and Health Education

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 Business Development Co-ordinator (in the role of **IT Co-ordinator**)

The IT Co-ordinator has a key role at the school. They are the key communicator between the school and the school's appointed **IT Support provider**; NetTechnical Solutions 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.

(a) 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 NetTechnical Solutions.

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. 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 NetTechnical Solutions 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.

7. 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 are not permitted to take videos and digital images at school events. All programmes of events in the Menuhin Hall include a line reminding the audience that it is prohibited to take photographs and videos.

Staff and volunteers are allowed to take digital / video images on behalf of the school but must follow this policy, the IT Acceptable Use Policy and the Staff Code of Conduct concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment 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.

Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (see Image Consent Form (available in Annex B)).

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images.

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 school's IT support company; NetTechnical Solutions 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 Business Development Co-ordinator.

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.

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. 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.

9. 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.

10. 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 (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.

11. 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 school's IT

support company; NetTechnical Solutions 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 Business Development Co-ordinator.

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. 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.

9. 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.

10. 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.

11. 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 Cheryl Poole, 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: _____

Revision History

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

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

Upon joining the school, all pupils are provided with a school email address which gives them access to their Microsoft 365 A3 licence. This licence grants the pupils access to a wide range of Microsoft applications which support them in their academic and music studies. Of note are Microsoft Teams, Microsoft Word, Outlook & OneDrive.

Each A3 licence grants pupils' access to both the web applications and allows the download of the Microsoft Office Suite (Word, PowerPoint, Excel) on to one device of their choosing. 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 encouraged to store all their schoolwork on their 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 email account.

All pupils 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.

2. 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 (Music 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 16+ app and the school therefore strongly discourages all pupils under 16 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 students being in possession of each other's personal phone numbers. To support this, the Music 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 Music House and Harris House duty phone do not use this app for communication.

3. Monitoring Use of IT

The School filters and monitors pupils' use of the School internet network via Smoothwall software. 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.

4. 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.

Advice for International Parents For international parents, we encourage parents to consider purchasing 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 (6am-11pm) 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.

5. Wi-Fi / 4G / Mobile Data

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. 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.

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.

The school does its utmost to ensure pupils are protected whilst browsing the internet, however 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 data after 11pm).
Whilst having some data is useful for when pupils are 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 does not have a UK-Sim, you will potentially see an extra charge for “data roaming” which happens when you use mobile data but are unable to connect to your network provider’s home country.

6. 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)

7. 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)
16GB RAM
256 / 512GB SSD (storage)

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.

Some pupils may be interested in working on Music technology and the school is building infrastructure to support this.

The school’s internet and devices are protected by a combination of a firewall for security, and an additional layer of age-appropriate filtering. Smoothwall is a school-specific provider of internet filtering, and one of the leading providers in the U.K. Sophos… Both systems are managed by NetTechnical Solutions, our IT support providers.

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.

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)

Appendix B: Image Consent Form

I understand that images in either photographic or video format may be taken of my child for internal use within the School, in order to fulfil the legitimate business interests of the Data Controller (The Yehudi Menuhin School, Stoke d'Abernon), including:

- For internal records/security/identification of pupils
- For teaching purposes (i.e., to demonstrate and improve on technique)
- For teacher observation purposes

I hereby detail below my instructions as to how I wish these photographs to be used externally:

PURPOSE	**CONSENT GRANTED? (Please tick YES or NO)**
For display on School premises:	YES ☐ NO ☐
For use on The Yehudi Menuhin School/Menuhin Hall websites:	YES ☐ NO ☐
For use on other affiliated websites:	YES ☐ NO ☐
For use in The Yehudi Menuhin School external publications: (e.g. Newsletter & Prospectus)	YES ☐ NO ☐
For use in reports to donors:	YES ☐ NO ☐
For use on the School's social media accounts:	YES ☐ NO ☐
For use in publicity/advertising material for internal and external performances (both in print and online):	YES ☐ NO ☐
For use in concert programmes (both on and off site):	YES ☐ NO ☐

* Where images are shared, there will be no captions detailing full pupil names unless the information is already in the public domain, as in the case of external competitions or promotional material. First name and initial of surname may be used and year group.

Please note that the School premises can be used by private hirers during non-School hours.

DECLARATION

I understand that I can change my instructions regarding consent at any time by contacting the Registrar, Marcia O'Mahony, at registrar@menuhinschool.co.uk or 01932 584795. or 01932 584795.

PUPIL NAME	
PARENT NAME	
PARENT SIGNATURE	
DATE	