Technology and E-safety Policy

1 Overview

1.1 E-Safety refers to the safe and responsible use of all Internet technologies and electronic communications such as computers, laptops, mobile phones, iPads and any other handheld devices that students might access.

1.2 This policy highlights and reinforces the need to educate students about the benefits and risks of using technology, and provides safeguards and raises awareness for users to enable them to control their online experiences. Each school has clear, age-appropriate 'Technology Use Guidance', which is shared and regularly reinforced with students (see Appendix 1).

1.3 This policy will operate in conjunction with other school policies including those for ICT, Behaviour, Bullying, PSHCE and Child Protection.

2 Guiding Principles

2.1 We embrace new technology wherever it supports our mission. Staff are confident users of technology and are encouraged to be innovative. Students use technology to inquire, communicate and safely take risks. When they move on from the School, they are confident users of current technology in a range of contexts, understanding the benefits, limitations and risks associated with its use.

2.2 A range of IT devices, software and Internet-based resources are used to support teaching and learning across the school where they enrich the learning experience, for example by:

- Improving access to the curriculum
- Encouraging collaboration between students
- Enhancing communication by enabling multimedia approaches
- Enabling authentic student research
- Supporting student self-management and organisation

2.3 Benefits of using the Internet in education include:

- Access to up-to-date information from a wide variety of sources
- Access to online educational resources
- Educational and cultural exchanges between students world-wide
- Access to experts in many fields for students and staff

3 Objectives of This Policy

3.1 This Policy sets out who in the organisation will have access to the Internet through the school network and how that access will be managed, along with the associated risks. It should be read in conjunction with the Student Code of Conduct, Student Misbehaviour and Sanctions Policy, Anti-Bullying Policy, Child Protection Policy, Personal Data Protection Policy and the Photo and Video Policy.

3.2 Further guidance for Staff use of Information Technology is available on the Staff Portal. In particular staff should be aware of The Staff Handbooks (Including the Code of Conduct for Staff and Guidance on Staff use of ICT and the Internet) and Communications Guidelines and

Protocols (including the 'Email Policy and Communications to Parents' and 'Social Media Protocol').

4 Teaching and Learning

4.1 How Internet access is managed within the School

4.1.1 The school Internet access has been designed for student and staff use and will include filtering appropriate to the age of the students and the needs of staff.

4.1.2 Students will be taught what Internet use is acceptable and what is not and will be given clear objectives for it safe use.

4.1.3 Staff will guide students in online activities that will support the planned learning outcomes, with due regard for the students' age and maturity.

4.1.4 Students will be educated in the skills of Digital Literacy i.e. the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Students will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

4.1.5 Infant and Junior Internet access must be approved and will be supervised at all times.

4.1.6 Senior students will be provided access according to requirements

4.1.7 All use should be in accordance with the relevant schools' Technology Use Guidelines (see Appendix 1).

4.1.8 Students must follow the procedure for reporting unsuitable Internet content.

4.1.9 This procedure will be shared with all students by their class teachers as part of the curriculum.

4.2 Remote Learning – Audio and Video Conferencing

4.2.1 If it is not possible for students to access the school campus, the School may activate 'Remote Learning' for students. At these times, teachers will use the online learning platforms that students are familiar with. This will ensure that students continue to be supported by their teachers, whilst undertaking meaningful learning tasks.

4.2.2 Conference calls may also be used when Remote Learning is activated, to enable real time voice or video communication between teachers and students. The School acknowledges that this can create situations where professional and personal boundaries are disrupted. This policy, and the further guidance for staff, parents and students in Appendix 2 aim to ensure that the various technologies available can be used in ways that are effective and safe for everyone.

4.2.3 The School expects staff, parents and students to adhere to the guidelines concerning appropriate dress, physical settings and behaviour detailed in Appendix 2. Teachers may terminate a student's participation in a video call if they have any concerns about that student's dress, location or behaviour.

4.3 Video Conferencing and Child Safety

4.3.1 Where video conferencing is used as a learning tool in the remote learning environment, classes may be recorded. Recordings produced in the remote learning environment are focused on capturing the teacher's presentation of material with the purpose of:

- Providing access to learning material for students who may miss the class in real time.
- Providing transparency around professional practice for the teacher.

4.3.2 The School will ensure that students and parents are informed about and consent to participate in classes that will be recorded.

4.3.3 All conference calls should be scheduled meetings, set up by a teacher. Teachers must not accept video calls – or accept online meeting invitations - from students or parents.

4.3.4 For Infant and Junior School children, meeting invitations will be sent via a parent's email address (as listed in the School Management System); an adult must be physically present with the student for the duration of the meeting.

4.3.5 For Senior School students meetings may be initiated via the students' email address. Teachers may choose to conduct 'audio only' meetings (no video),

4.3.6 Teachers are encouraged to make use of screencasting and pre-recorded video to share instructions and explanations through the online learning platforms outside of live video calls.

4.3.7 Class teachers and subject specialists will not conduct video calls with individual students as part of the remote teaching and learning provision. However 'one to one' meetings with students may be required for specific purposes, such as:

- a wellbeing check in with a school counsellor or safeguarding officer
- an individual assessment required by an external examination board
- an individual instrumental music lesson

In these cases either an audio recording, or a recording of the teacher's screen along with audio, must be made in accordance with 4.3.1.

4.3.8 Reporting and management of safeguarding and child protection concerns is guided by the Safeguarding and Child Protection Policy. In particular:

- Any safeguarding concerns about students should be discussed with Designated Safeguarding Lead staff.
- Any concerns about inappropriate behaviour by staff should be discussed with Designated Safeguarding Lead staff, a Head of School or the Director of Human Resources.
- Any concerns about misuse of personal information, manipulation, reproduction or circulation of remote learning images or recordings should be reported to Designated Safeguarding Lead staff.
- Any staff who may be concerned that they have inadvertently behaved in a manner, or said something, that could be misinterpreted or raise concerns about their professional integrity should create transparency around the concern by consulting with Designated Safeguarding Lead staff.

4.4 How e-safety issues are handled

4.4.1 Any breach of the Technology Use Guidance, or the Student Code of Conduct will be dealt with according to the Behaviour Policy.

4.4.2 Cyber-bullying incidents are taken extremely seriously and are dealt with in the same way as any other incidence of bullying (see the Anti-Bullying Policy).

4.4.3 Disciplinary action may be taken where a staff member's use of technology is in breach of the Code of Conduct for Staff (see Faculty Staff Handbook and Business Support Staff Handbook). The staff handbooks for faculty and support staff include more detailed expectations for the appropriate use of technology.

4.4.4 Any concern that an e-safety incident may be an indicator of a child protection issue must be reported to the relevant Designated Safeguarding Lead in line with the Safeguarding and Child Protection Policy.

5 Managing Information Technology

5.1 How our IT system security is maintained

5.1.1 The School IT systems will be reviewed regularly by the EBT director and the EBT team with regard to security.

5.1.2 Security strategies will be discussed and agreed between the department of Educational and Business Technology (EBT) and all school departments – security issues will be raised at the Technology Working Group (TWG), for faculty departments and at the COO Meeting for Business Support departments. Urgent or high-level concerns will be raised directly with the Management Team.

5.1.3 In the event of a security breach, the EBT director has the authority to take whatever action they see fit in order to minimise the risk to the School, including temporarily shutting down or restricting access to the network.

5.1.4 Security measures will include but are not limited to the following:

- All staff members will be required to use strong passwords and to change them regularly.
- Separation will be maintained between the guest network and the internal network domains. Virus protection software will be installed on all School PCs and updated regularly.
- An Internet firewall will be maintained to screen all incoming traffic.
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to email.
- Files held on the School's network will be regularly checked for appropriate content.
- The Network Manager will ensure that the system has the capacity to take the expected traffic caused by Internet use.

5.2 How electronic communication is managed

5.2.1 Each student in the Junior and Senior Schools has access to their own school-based email account, which is specific to their system login.

5.2.2 Students are able to send emails internally and externally for school use, under supervision and/or appropriate guidance.

5.2.3 Student emails can be accessed at the request of a subject or class teacher with permission from a member of the Leadership Team of the relevant school.

5.2.4 All staff are issued with a 'tts' email address, which should be used for all school-related communication. Staff are expected to follow the Email Guidance published by the Communications Team and must take note of the 'principles of responsible use' of ICT included in the staff handbooks.

5.3 How public access online content is managed

5.3.1 Personal information of staff, parents or students is collected, used and disclosed in accordance with our Personal Data Protection Policy.

5.3.2 The Public website will include the school address, and the email addresses and telephone numbers of the school offices and the main reception, admissions department, the communications department and the development department.

5.3.3 The Committee for Private Education Singapore (CPE) requires faculty staff names and academic qualifications on the public website. These are published alongside staff photographs.

5.3.4 Photographs and video of students will be used on the public website, in online newsletters and on social media in accordance with our current Photo and Video Policy. Students' full names will not be used on public websites when associated with photographs, or in any way which may be to the detriment of students.

5.3.5 The Communications department will take overall editorial responsibility for the public website and the Parent Portal, ensuring that content is accurate and appropriate on all pages directly related to the day-to-day workings of the School.

5.3.6 The School has an official presence on social media. Staff are expected to follow the current Social Media Guidelines issued by the Communications Department when posting on social media, whether using their personal accounts or an official school account.

5.3.7 The copyright of all material published on the public website, online newsletters and social media must be held by the School, or be attributed to the owner where permission to reproduce has been obtained.

5.3.8 School-managed student blogs will be password protected or run from the School intranet sites.

5.4 How emergent Internet technologies are managed

5.4.1 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the School is allowed.

6 Cloud Storage

6.1 Benefits of and concerns regarding cloud storage solutions

6.1.1 We encourage the use of cloud services for file storing and sharing. Cloud storage of files can expedite collaboration and sharing of information anytime, anywhere, and with anyone. However, there are a number of information security and data privacy concerns about use of public cloud storage (Microsoft SharePoint, OneDrive, and Google Drive) services at the School. They include the following:

- The School can no longer guarantee the quality of access controls protecting the data
- The location where the data is stored may not be known
- Using cloud storage client software to synchronise files between work and personal devices could result in sensitive information being held inappropriately on personal equipment.

6.1.2 This policy is designed to maximise the benefits of using cloud storage whilst minimising the risks, by identifying the kind and type of School information that is appropriate for storing and sharing using these services.

6.2 **Storage of information**

6.2.1 The School only supports business-oriented cloud storage services such as Google Drive and Microsoft OneDrive for Business.

6.2.2 Confidential information, such as personal biodata of staff or students, or other sensitive information (e.g. HR- or finance-related information) should be maintained in secure School systems and not stored in cloud-based drives.

6.2.3 Documents that need to be retained long-term, such as templates and policy documents, should be stored on SharePoint or shared network drives, rather than on personal cloud drives (OneDrive, Google Drive, etc.).

6.2.4 Staff are strongly advised to keep more than one copy of important documents.

6.2.5 Staff should ensure that there is a suitable level of authentication on any mobile or portable device used to download any school-related data from cloud storage. Such a device must be password protected.

6.3 Sharing files and folders

6.3.1 Where there is a requirement to share information with others, it is important that individuals who enable the sharing of data do so with the following safeguards:

- Grant access only to the specific folders and files that are required to support the collaboration or information sharing. Ensure that no other folders or files are made available.
- Take care to ensure access is granted to the right individuals.
- Staff sharing information through cloud services have a responsibility to ensure that all collaborators are aware of any privacy or confidentiality issues.
- Remove individuals when they no longer require access to files or folders.

6.4 Synchronising between devices and cloud services

6.4.1 Synchronising information to and from cloud storage is not necessary, however it can provide significant advantages in terms of information availability and speed of access in circumstances where the user will be off-line. Synchronising information across devices requires the following safeguards:

- Devices involved in the synchronisation process must be protected from loss and unauthorised access. Mobile devices must have a “PIN” code or equivalent security enabled.
- Devices involved in the synchronisation process must be protected from malware and kept up to date with operating system security patches.

7 Internet Filtering Policy

7.1 We have a duty of care to ensure the safety of our community. This applies equally to both the physical and virtual environments. As such, the School uses web-filtering technologies to prevent access from devices to particular types of Internet content.

7.2 The filtering technologies aid in the **security and stability of the network** by preventing the download of software that is malicious and/or disruptive or could impact significantly on the performance of the network.

7.3 In addition, the filtering technologies **restrict access to material** that is classified by the Leadership Team as **objectionable or inappropriate**.

7.4 All users are reminded that the web-filtering policy is not a total guarantee of web safety and is complemented by the appropriate responsible use agreement and on-going education in digital citizenship.

7.5 **Current Filtering Guidelines**

7.5.1 At present the Leadership Team has agreed to the following guidelines:

- Where possible enforce Safe Search in web search engines
- Restrict access to websites that fall under the following categories (as defined by the filtering software)

• Abortion • Adult mature / content • Alternative spirituality / belief • Chat / IM / SMS • Child pornography • Controlled substances • Extreme • Gambling • Games • Hacking	• Humour / jokes • Intimate apparel / swimwear • Malicious websites • Marijuana • Nudity • Peer to peer • Personal / dating • Phishing • Piracy / copyright concerns • Pornography • Proxy avoidance	• Scam / questionable / illegal • Sex education • Sexual expression • Social networking • Spam • Suspicious • Violence / hate / racism • Weapons

7.6 Filtering Order

7.6.1 It is not uncommon for a site to be classified under more than one **category by the Internet filters. In such instances, the logic of the Internet filters is to apply the more restrictive policy first.** For example, if a site was classified as "games" and also "education", the site would be blocked by the "games" rule as that is applied before the "allow education sites" rule.

7.7 Process for allowing/blocking access to an individual site

7.7.1 If a teacher requires an individual site to be blocked or unblocked for legitimate educational purposes, then they should submit an email to EBT Help Desk requesting access and a very brief overview of the reasoning. This is for record keeping purposes only. A log of the requests will be available for the Leadership Teams of each school to review.

7.7.2 Such examples have included access to certain alcohol and sex education websites for the purpose of PSHCE lessons.

7.7.3 Staff should be aware that intentionally attempting to circumvent our filtering policy could expose the network to security risks and will be treated as a breach of the Code of Conduct.

7.8 Process for review of the categories or policy

7.8.1 We will continually review the categories and may implement different filtering policies for different year groups, where appropriate.

7.8.2 If a staff member wishes to have the categories or policy reviewed, they should first approach the Leadership Team of their individual school.

7.8.3 If the Leadership Team of the school concerned approves the request, it would then be submitted to the Director EBT to be implemented, subject to any technical issues.

7.8.4 If there is a technical issue that prevents immediate implementation, for example if EBT is concerned over the security of the network, or if there are implications for the other schools, options would be investigated for discussion.

7.8.5 Any change that will affect the whole school must be discussed by the TWG and approved by the whole school Leadership Team.

8 Communication of This Policy

8.1 How E-safety is introduced to students

8.1.1 Awareness of E-safety and the importance of safe and responsible Internet use are taught explicitly, through our PSHCE and Computing curricula. These planned curricula aim to introduce issues and strategies, at an age-appropriate level, for staying safe and will bear in mind the increasing access to technology as students progress through the School. The curricula materials are reviewed regularly and draw on available expert advice, particularly from commonsense media (https://www.commonsensemedia.org/educators)

8.1.2 The Responsible Use Guidelines (Appendix 1), including Internet safety advice, are incorporated into the Code of Conduct for Students and are prominently displayed around the School. For Senior and Junior students, the Responsible Use Guidelines will also be available on the School's intranet sites.

8.1.3 Students will be informed that Internet use is monitored and logged and that these logs can be retrieved under the direction of a Head of Year or member of Senior Management Team.

8.1.4 Instruction in responsible and safe use will precede Internet access.

8.2 How the policy is discussed with staff

8.2.1 All staff will be made aware of the School Technology and E-Safety Policy and its application and importance explained.

8.2.2 Staff should be aware that Internet traffic can be monitored and traced to the individual user.

8.2.3 Staff should be aware that school email can be retrieved and opened under the written direction of the relevant Head of School or CEO; discretion and professional conduct is essential.

8.3 How parents' support is enlisted

8.3.1 Parents' attention will be drawn to this policy in our newsletters, brochure and on our website.

8.3.2 E-safety-related incidents will be handled sensitively to inform parents without causing undue alarm.

8.3.3 A partnership approach with parents will be encouraged. This will include parent information sessions and newsletter articles to explain how technology is being used in the School and suggestions for safe Internet use at home.

9 Role of Governors

9.1 The role of the Education Sub-Committee of the Board of Governors (ESC)

9.1.1 The role of the ESC is to be aware of the School's approach to E-Safety and of how this policy relates to more general policies on behaviour and child protection, as well as the PSHCE (Personal, Social, Health and Citizenship Education) curriculum.

9.1.2 Any changes to this policy must be approved by the ESC.

Appendix 1

Technology Use Guidelines - Infant School

We are Principled Users of Technology

When I Use Technology

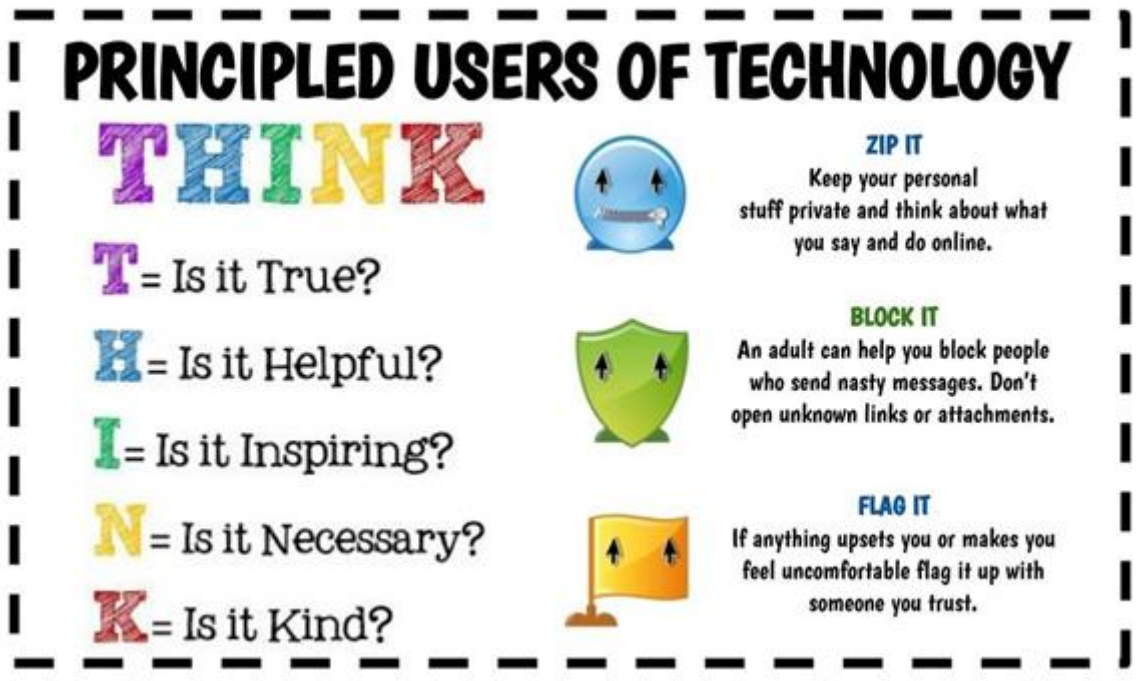
- I will only use technology within lessons and will not bring my own devices to school.
- I will only use apps and websites that the teacher has instructed me to use.
- I will always ask an adult for permission before using the internet.

Staying Safe and Being Responsible

- I will keep my personal details such as my password, full name, parent phone number, birth date and home address private (ZIP IT).
- I will only post/share images, videos and learning which are:
  True, **H**elpful, **I**nspiring, **N**ecessary and **K**ind.
- I will only open, edit or delete my own work and will respect the work created by others.
- If I accidentally find anything that worries me, upsets me or I think is unpleasant, I will tell an adult (FLAG IT) and not share what I have seen with other children.

Consequences

- I know that my use of technology will be monitored and that my parent/ carer will be contacted if a member of staff is concerned about my e-safety.
- I understand that the use of technology can be withdrawn for a period of time if I do not follow these guidelines.



Technology Use Guidelines - Junior School

Principled, Caring Communicators

When I Use Technology

- I will only use technology in school for school learning tasks.
- I will only use technology when I have been asked by my teacher.
- I will only bring my phone to school if I need it to contact my parents after CCAs. It will stay in my bag on silent during the school day.

Staying Safe and Being Responsible

- I will be responsible for my behaviour when using technology because I know that these guidelines are to keep me safe.
- I will protect my identity, and that of others, by not sharing personal information online such as names, phone numbers, addresses, passwords or the name of the school.
- I will only open/edit/delete my own files.
- When working on collaborative documents e.g Google Docs or Google Slides, I will only edit or delete my own work.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- If I accidentally find anything inappropriate whilst online, I will tell my teacher immediately.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I will not record or publish audio or video of myself or any member of the community unless they have given me permission and I have been instructed to do so by a teacher.

Communication

- I will only use my school e-mail address for school-related activities.
- I will make sure that all electronic communication with other children and adults is responsible, polite and sensible.
- I will only open e-mail attachments from people I know, or whom my teacher has approved.
- I will follow age restriction guidelines for social media. If I do have access to these applications, it is with my parent/guardians full understanding and guidance. I will not use any social media in school.

Consequences

- I know that my use of technology can be checked and that my parent(s) will be contacted if a member of the school staff is concerned about my e-Safety.
- I understand that the use of technology can be withdrawn for a period of time if I do not follow these guidelines.

iPad Usage

- I understand that the use of iPads in lessons is at the choice of each teacher.
- I will only use my iPad when asked to by a teacher.
- I will not use my iPad before or after school or during break times unless working with a teacher.
- I will not use my iPad on the school bus.
- I will not use group messaging e.g. iMessage/WhatsApp/Google Docs to talk to groups of children on my iPad, as I understand this can upset others and make people feel left out.

Technology Use Guidelines - Senior School

Principled, Caring Communicators

When and Where I Use Technology:

I will use technology and online tools responsibly and respectfully, to support my learning

Learning devices:

- I will bring my device fully charged to lessons, along with keyboard, stylus and ear/headphones
- I will keep my device turned off, closed and screen down until directed to use it by a teacher
- I will have all notifications and alerts turned off during school hours
- If I want to use my device for work at break and/or lunchtime then I will go to the library
- Sixth Form students may use their devices for work in the Well Bean cafe
- Students on study leave may use their devices in the red/white cafe immediately before an examination

Phones:

- I will keep my phone in my locker and on silent mode during school hours.
- I may use my phone as I exit the school at the end of the of the day to communicate with parents/book a taxi
- Sixth Form students may use their phones on Level 4 of the Sixth Form Centre

Ear/Headphones:

- I will remove ear/headphones immediately upon entering the school site and will only use them again when directed to do so by a teacher during a lesson or when doing private study in the library

Gaming/Messaging/Social Media/YouTube

- I may not access gaming, messaging or social media apps or websites anywhere on site at any time
- I will only access YouTube as part of directed learning in lessons

After school

- I understand that after school I should either be going home, in a CCA or waiting for a CCA to start
- If waiting for a CCA, I understand that I must go to the library

The Library

- The library is the only place I may use my personal learning device outside of lesson time
- ALL the above rules also apply to the library ie phones not allowed

Safe and Responsible Use:

- I will protect my identity, and respect that of others, by not sharing personal information online such as names, phone numbers, addresses, passwords or the name of the school
- I will only record, upload or distribute audio, images or video of myself or any member of the community with the agreement of the people involved and when instructed to do so by a teacher as part of a learning task
- I will only look for, create, contribute to, save or distribute appropriate material and will report anything inappropriate that I find to my Head of Year
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I will be a principled learner when using online resources and will always credit other people's work
- I will respect the school server and wireless network settings and filters and not use a VPN or hotspot to bypass these

Consequences

- I understand that my use of technology is monitored and that a breach of these rules will have consequences
- I understand my device/phone/headphones will be confiscated if I choose to ignore any of the rules above

1st Infringement	Negative iSams/ Device confiscation until 3.15pm
2nd Infringement	Negative iSams/ Device kept overnight AND Detention with Mrs Anderson-Au/Mr Allan/Mr Goodliffe
3rd Infringement or more	Meeting with parents

Appendix 2

Guidance for Teachers, Students and Parents for the use of Video Conference Calls

General

The School acknowledges that the use of video conferencing tools creates a situation where professional School-Family relationships intersect with personal environments. The following guidance is intended to ensure that the experience is effective and safe for everyone.

Parents are encouraged to assist their children in building healthy personal boundaries by ensuring that their children are appropriately dressed for any learning involving video conferencing, and that they are able to participate from a suitable location.
Students are not expected to be in school uniform. Clothing should be in line with what would be deemed appropriate for a school mufti day. Pyjamas, swimming costumes or other overly revealing clothing are not acceptable.

The School recognises that students, particularly in the Senior School, are likely to have desks in their bedrooms where they study and this may seem a logical place from which to video conference with their teachers. Bedrooms are however, considered highly personal environments. In accordance with the School's commitment to educating students about appropriate personal boundaries, the School discourages students from using their bedrooms as locations for remote learning video conferencing.

The School recommends that students participating in video conferencing:
- Use family spaces rather than private spaces.
- Consider using digital tools that blur or obstruct backgrounds to protect their family's privacy where these are available.

Staff, parents and students should all take care that any setting visible to others on the call
- Does not contain material that any reasonable person would find offensive in relation to race, religion, culture or gender, or any otherwise inappropriate material.
- Does not contain any highly personal items or information that may allow unreasonable line of sight into personal life.

School Specific Guidance:

Infant School

Teachers:
- You must not accept any meeting requests from parents or children. All class meetings should be initiated from a link via email, set up by the teacher, and sent from the teacher's TTS email address.
- In terms of safeguarding, if you see anything concerning during the meeting, please follow safeguarding procedures as you would in school.
- As a Host, please use a school provided device when video conferencing.
- You must not record or capture images from any video conferencing sessions.
- Any video conferencing should be scheduled rather than ad hoc video call connections.
- Please ensure you are dressed professionally, even if working from home.

- Please ensure that your background does not compromise your privacy or location – as an alternative a virtual background is available within the Zoom software.
- Please ensure you are never one-to-one on Zoom with a child – in a group conference, if you suspect a child is unsupervised, you have permission to exit them from the meeting.
- Please begin each conference with a reminder about expectations during the meeting. Pre-set your meeting to mute children's microphones to start while you introduce and set out the expectations in line with our technology use guidelines. Use hands up initially for children to indicate that they would like to share something.
- You must disable the chat function.

Parents:

- Please ensure your child and any others in the household who may be visible during the conference are appropriately clothed.
- The device used must be set up in a communal room and an adult must always be present during the conference – teachers reserve the right to remove any child who they believe to be alone.
- Please ensure that the background visible behind your child does not compromise your privacy or location – as an alternative a virtual background is available within the Zoom software.
- Please note that these conferences are specifically for children and their teacher to catch up – if you need to speak to the teacher, please arrange an appropriate time via email and please respect the privacy of other children who may contribute during the call.
- Please note that recording or image capturing of the conferences is not allowed.
- Please be advised that minors under the age of 18 are not permitted to create personal Zoom accounts under the terms of service.

Children

- You must always have a grown up in the room when you are using an internet connected device.
- Make sure you are fully dressed.
- Remember, we should communicate online in exactly the same way as if we were talking face to face. THINK before you speak.
- Follow the same rules as when you are in school. Hands up and don't shout out. (Remember you will be on mute to begin with and the teacher will allow you a turn to speak)
- We expect the same outstanding standards of behaviour as when you are in class.
- You must not record or take photos of the video session.

Junior School

Teachers

- You must not accept any meeting requests from parents or children. All class meetings should be set up by the teacher, using the teacher's tts email address.
- In terms of safeguarding, if you see anything concerning during the meeting, please follow safeguarding procedures as you would in school.
- Please use a school provided device when video conferencing
- You must not record or capture images from any video conferencing sessions
- Any video conferencing should be scheduled rather than ad hoc video call connections.

- Please ensure you are dressed professionally, even if working from home.
- Please ensure that your background does not compromise your privacy or location – as an alternative a virtual background is available within the Zoom software.
- Please ensure you are never one-to-one on Zoom with a child – in a group conference, if you suspect a child is unsupervised, you have permission to exit them from the meeting.
- Please begin each conference with a reminder about expectations during the meeting. Pre-set your meeting to mute children's microphones to start while you introduce and set out the expectations in line with our technology use guidelines. Use the hands up feature initially for children to indicate that they would like to share something. Use the teacher guidance for setting up Zoom

Parents

- Please ensure your child and any others in the household who may be visible during the conference are appropriately clothed.
- The device used must be set up in a communal room and an adult must always be present during the conference – teachers reserve the right to remove any child who they believe to be alone.
- Please ensure that the background visible behind your child does not compromise your privacy or location as all participants in the conference will be able to see your child and his/her surroundings – as an alternative a virtual background is available within the Zoom software.
- Please note that these conferences are specifically for children and their teacher to catch up – if you need to speak to the teacher, please arrange an appropriate time via email and please respect the privacy of other children who may contribute during the call.
- Please note that recording or image capturing of the conferences is not allowed.
- No recordings will be made by the school of the video conferences and all images transmitted will be for the purpose of carrying out the video conference then in session. By joining in, you will be consenting to the disclosure and use of any of your and your child's personal data (which includes images) which may be transmitted during the video conference.
- Please be advised that minors under the age of 18 are not permitted to create personal Zoom accounts under the terms of service.

Students

- Using Zoom at home
- Remember, we should communicate online in exactly the same way as if we were talking face to face. THINK before you speak.
- Make sure you are fully dressed.
- Follow the same Responsible Use Guidelines as you would in school.
- You must always have a grown up in the room when you are using video.
- We expect the same outstanding standards of behaviour as when you are in class.
- You must not record or take photos of the video session.

Senior School

Teachers

- You must not accept any video meeting requests from parents or students. All class meetings should be set up by the teacher, using the teacher's tts email address.
- Any video conferencing should be scheduled rather than ad hoc video call connections.

- In terms of safeguarding, if you see anything concerning during the meeting, please follow safeguarding procedures as you would in school.
- Please use a school provided device when video conferencing
- Please ensure you are dressed professionally, even if working from home.
- Please ensure that your background does not compromise your privacy or location – as an alternative your background can be blurred in Teams software
- Avoid one-to-one video calls with students unless you are conducting an assessment that can only take place one to one such as a Languages oral or an IA*. If only one student has joined a scheduled class call, please terminate the call and reschedule.
- Please remind students that normal school expectations of behaviour apply during a remote learning session.

*Where one to one sessions are required, parents must have given separate, specific permission and an audio recording must me made, for safeguarding purposes.

Students

- Remember, we expect the same standards of behaviour in a class video meeting as we do during normal lessons.
- Make sure you are fully dressed in clothing that would be appropriate for a mufti day in school.
- Follow the same Responsible Use Guidelines as you would in school.
- You must not make any recording of the video during the meeting. Your teachers will share any material that you need with you separately.

Parents

Please note that these conferences are specifically for the teacher to address learning issues with the class. If you are in the room with your child, please remain a silent observer of the meeting and respect the privacy of other students.

- All images transmitted during video conferences will be used for the purpose of carrying out the video conference then in session. A recording will be made of each session for safeguarding and record purposes, and stored on a school managed site.
- By allowing your child to join in the video call, you will be consenting to the disclosure and use of your, and your child/children's personal data (which includes images) which may be transmitted during the video conference and simultaneously recorded